I-Gear®

Version 3.5

Software Manual

for Microsoft® Windows NT® Server 4.0,
Red Hat® Linux® 5.2 or later,
Sun® Solaris® 2.x Systems,
Check Point™ FireWall-1®,
and Microsoft Proxy Server

Copyright © 1996-2000 Unified Research Laboratories, Inc., a Symantec company. All rights reserved.

All of the documentation and software included as a part of the I-Gear software package is subject to the URLabs License Agreement and Limited Warranty provided with the package. Usage or copying of the software or documentation except as permitted by the License Agreement is unlawful.

IGSM35-1 Printed in USA 1/00

Software version I-Gear 3.5

Unified Research Laboratories, URLabs, I-Gear, Mail-Gear, Mail-Gear Web Client, PowerAdmin, Dynamic Document Review, AutoLock, AutoAlert, Audit Mode, "Defining the Role of Content Management," and the URLabs, I-Gear, and Mail-Gear logos are trademarks or registered trademarks of Unified Research Laboratories, Inc., in the United States and other countries. Geared for Learning is a service mark of Unified Research Laboratories, Inc., in the United States and other countries. Sun, Sun Microsystems, the Sun logo, Solaris, Java, and Netra are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. SPARC is a registered trademark of SPARC International, Inc. Products bearing SPARC trademarks are based on an architecture developed by Sun Microsystems, Inc. Apple and Macintosh are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. Microsoft, Windows NT, and/or other Microsoft products referenced herein are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Netscape Navigator is a registered trademark of Netscape Communications Corporation in the United States and other countries. Red Hat is a registered trademark of Red Hat Software, Inc., in the United States and other countries. Linux is a registered trademark of Linus Torvalds. FireWall-1 and Check Point are trademarks or registered trademarks of Check Point Software Technologies Ltd. Intel and Pentium are registered trademarks of Intel Corporation. All other trademarks are the sole property of their respective owners.

URLabs Software License Agreement and Limited Warranty

READ THIS DOCUMENT CAREFULLY. THIS IS A LEGAL AGREEMENT BETWEEN YOU AND UNIFIED RESEARCH LABORATORIES, INC. ("URLABS"). BY USING THIS SOFTWARE ("SOFTWARE") AND THE DOCUMENTATION ACCOMPANYING THIS SOFTWARE ("DOCUMENTATION"), YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT, INCLUDING WITHOUT LIMITATION THE DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITY CONTAINED HEREIN. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS AGREEMENT, DO NOT USE THIS SOFTWARE AND PROMPTLY RETURN IT TO THE PLACE WHERE OR TO THE PERSON FROM WHOM YOU PURCHASED IT.

The enclosed Software and Documentation are licensed, not sold, to you by URLabs. You shall inform all users of the Software of the terms and conditions of this Software License Agreement.

1. GRANT OF LICENSE; USE RESTRICTIONS. URLabs grants you a personal, nontransferable, and nonexclusive right to install the Software on a single server for your own internal use. You shall not permit any other party to use the Software or process or permit to be processed the data of any other party; provided, however, that if you are an "Internet Service Provider," as hereinafter defined, you may install the Software on a single server to provide "ISP Services," as hereinafter defined.

> You are an "Internet Service Provider" if you are a firm, company, or organization that provides for a fee Internet access or services to your subscribers, none of whom are under your immediate employ or the employ of any parent, subsidiary, or affiliate firm, company, or organization.
>
> "ISP Services" means content-managed Internet access service and/or electronic mail service provided by you as an Internet Service Provider to your subscribers using the Software.

You agree that you shall not disassemble, reverse compile, reverse engineer, decrypt, reproduce, adapt, modify, translate, distribute, duplicate, copy, transfer possession of, loan, rent, lease, sublicense, resell for profit, create derivative works based upon, or make any attempt to discover the source code of the Software or any portion thereof.

The Documentation may be used for your internal use only. You may not duplicate, copy, or otherwise reproduce the Documentation nor may you distribute the Documentation to any third party.

Prior to disposing of any media or apparatus containing the Software or Documentation, you will ensure that any Software or Documentation contained on such media or stored in such apparatus has been completely erased or otherwise destroyed.

2. OWNERSHIP. You agree that no title to the Software or the Documentation, or to the intellectual property in any of the Software or Documentation or in any copy of the Software or Documentation, is transferred to you, and that all rights not expressly granted to you hereunder are reserved by URLabs.

3. LIMITED WARRANTY. URLabs warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that URLabs will replace any defective media returned to URLabs within the warranty period. This Limited Warranty is void if failure of the Software media has resulted from accident, abuse, or misuse of the media. URLabs does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

4. DISCLAIMER OF WARRANTIES. THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR PARTICULAR PURPOSE, OR NONINFRINGEMENT. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE IS WITH YOU.

5. LIMITATION OF LIABILITY. IN NO EVENT SHALL URLABS BE LIABLE TO YOU FOR ANY DAMAGES WHATSOEVER, INCLUDING WITHOUT LIMITATION LOSS OF DATA, USE, PROFITS, OR GOODWILL, OR INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES ARISING FROM ANY CAUSE AND ON ANY THEORY OF LIABILITY INCLUDING WITHOUT LIMITATION CONTRACT, WARRANTY, STRICT LIABILITY, NEGLIGENCE OR OTHER TORT, BREACH OF ANY STATUTORY DUTY, PRINCIPLES OF INDEMNITY, THE FAILURE OF ANY LIMITED REMEDY TO ACHIEVE ITS ESSENTIAL PURPOSE, OR OTHERWISE, EVEN IF URLABS HAS BEEN NOTIFIED OF THE POSSIBILITY OF SUCH DAMAGES. THESE LIMITATIONS SHALL APPLY NOTWITHSTANDING THE FAILURE OF THE ESSENTIAL PURPOSE OF ANY LIMITED REMEDY, AND REGARDLESS OF WHETHER YOU ACCEPT THE SOFTWARE.

6. EXPORT RESTRICTIONS. You agree that you shall not directly or indirectly export the Software.

7. TERMINATION. This license is terminated if you fail to perform or observe any covenant, condition, or term to be performed or observed under this Agreement. URLabs, at its sole option, may provide written notification of the termination of the License for any reason, and in addition to any other rights or remedies available to URLabs, you

shall promptly return to URLabs the original and all copies of the Software and Documentation in your possession, in whole or in part, in any form, including partial copies or modifications, and within two weeks after any such termination you shall certify in writing to URLabs that you have done so through your best efforts and to the best of your knowledge.

8. U.S. GOVERNMENT RESTRICTED RIGHTS. U.S. GOVERNMENT RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19(c)(1) and (2) or subparagraph (c)(1) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and/or in similar or successor clauses in the FAR, or the DOD or NASA FAR Supplement, as applicable. Unpublished rights are reserved under the Copyright Laws of the United States. Contractor/manufacturer is Unified Research Laboratories, Inc., 1 Old Oyster Point Road, Suite 300, Newport News, VA 23602.

9. LAWS GOVERNING WARRANTIES AND LIABILITY. Some U.S. states do not allow the limitation or exclusion of liability for incidental or consequential damages, or allow the exclusion of implied warranties, so the above limitation and exclusion may not apply to you, and you may have other rights which vary from state to state. In any event, URLabs' liability shall not exceed the purchase price actually paid for the Software.

10. GENERAL. This Agreement shall be governed by and interpreted in accordance with the laws of the State of Virginia. You hereby submit to the jurisdiction of the District and Circuit courts for the city of Hampton, Virginia, and the U.S. District Court for the Eastern District of Virginia, Newport News Division, and agree that these shall be the sole fora to resolve all disputes arising under this Agreement or connected in any way with the Software. You agree to pay all costs associated with any such action or suit, including URLabs' costs and attorney's fees. This Agreement may only be modified by a written document that has been signed by both you and URLabs. If any provision of this Agreement is deemed invalid by a court of competent jurisdiction, it is to that extent to be deemed omitted, unless the court can modify said provision to make it valid and enforceable, in which case the provision shall be so modified. The remainder of the Agreement shall be valid and enforceable to the maximum extent possible.

Table of Contents

Welcome to I-Gear 1
Overview 1
Using this Manual 1
Notation Conventions in this Manual 2

The I-Gear Design 3
Proxy/Caching Feature 3
I-Gear Objects 4
I-Gear Methods 5
Hierarchy of Permissions 6
Hierarchy of Events 8

Understanding Filter Lists and DDR 9
Predefined Lists 9
Local Lists 13
List States 13
Adding URLs to Lists 15
Dynamic Document Review 16
How Filter Lists and DDR Work Together 18

I-Gear User Interface 25
The I-Gear Tool Bar 25
Sorting Feature for FTP 33

I-Gear Administration 35
Accessing the Administrative Functions 35
Standard (Default) Administrative Interface 37
Family Interface (Enterprise version only) 38
Global Administrative Permissions 39
Hierarchical Administration (Enterprise version only) ..40
Search Capability for Object Lists 44
Editing the Access Denied Page 47

Working with the Client Object 49
Adding a Client 49

Deleting a Client 50
Modifying a Client 51
Scheduling an Event for a Client 56
Generating a Report for a Client 71

Working with the User Object 79
Adding a User 79
Deleting a User 87
Modifying a User 88
Scheduling an Event for a User 95
Generating a Report for a User 96

Working with the Cast Object 99
Adding a Cast 100
Deleting a Cast 100
Modifying a Cast 101
Scheduling an Event for a Cast 104
Generating a Report for a Cast 104

Working with the List Object 105
Adding a List 105
Deleting a List 107
Modifying a List 107
Generating a Report for a List 112

Working with the Dictionary Object 115
Modifying a Dictionary 115
Generating a Report for a Dictionary 117

Working with the System Object 119
Modifying the System 119
Scheduling the System 135
Generating a Report for the System 136

Using I-Gear: Some Examples 141
Initial Setup (Configuring I-Gear) 141
Automated Policy Enforcement (Using AutoLock) 151
Monitoring Internet Access (Using Audit Mode

and AutoAlert) 154
Controlling Access (Scheduling Daily Events) 160
ISP Configuration (Setting Up Transparent Proxying, Client Revalidation, and Casts) 162

Index.....171

1. Welcome to I-Gear

This manual contains instructions for using the I-Gear version 3.5 software, hereafter referred to simply as I-Gear, as a stand-alone, multi-threaded caching proxy server for Sun Solaris version 2.5 or later, Red Hat Linux version 5.2 or later, and Microsoft Windows NT Server 4.0. The proxy server acts as a gateway to the Internet and, with I-Gear, can be used to review information passing to your internal LAN from the outside. I-Gear allows you to control all aspects of this information as it flows into your network. I-Gear 3.5 is also available as a transparent plug-in for either Check Point FireWall-1 for Sun Solaris version 2.5 or later and Microsoft Windows NT Server 4.0 OR Microsoft Proxy Server. Caching currently is not supported for I-Gear 3.5 for FireWall-1.

Overview

To ensure that you make effective use of I-Gear's capabilities, the following basic steps are recommended.

- Read "The I-Gear Design" on page 3, "Understanding Filter Lists and DDR" on page 9, and "I-Gear Administration" on page 35 carefully. Several concepts must be thoroughly understood in order to maximize I-Gear's effectiveness. Careful and thoughtful planning will give you the control you desire and will eliminate end-user confusion.
- Install I-Gear 3.5 on a server that meets the minimum requirements outlined in the *I-Gear Installation Guide*.
- Follow the procedures outlined in the *I-Gear Installation Guide* to initially configure I-Gear for your network. This manual contains guidance on establishing your default settings for filtering access to the Internet. **This step is extremely important because I-Gear is shipped with the default settings for all lists in the Off state. You must activate filtering.**
- Once you have established basic filtering with I-Gear, you can begin to refine your settings to suit your specific needs.

Using this Manual

This manual contains information on using I-Gear version 3.5. The manual is divided into 12 sections. The next two sections, "The I-Gear Design" and "Understanding Filter Lists and DDR," cover the design philosophy that makes I-Gear the leading Internet Content Management software. Section 4 introduces the I-Gear user interface, and section 5

provides an introduction to the I-Gear administrative interface. Sections 6 through 11 discuss in detail the various administrative functions. Section 12 contains some specific examples to demonstrate I-Gear's functionality. Finally, an index is at the back of this manual to help you find exactly what you need.

Notation Conventions in this Manual

Courier typeface is used to indicate text you will enter into specific fields. For example,

```
John Smith
```

Underlined Times typeface is used for clickable hypertext links. For example,

Visit the Symantec Corporation Home Page.

Boldface is used for selectable items such as buttons and text boxes. For example,

Click the **Modify** button.

2. The I-Gear Design

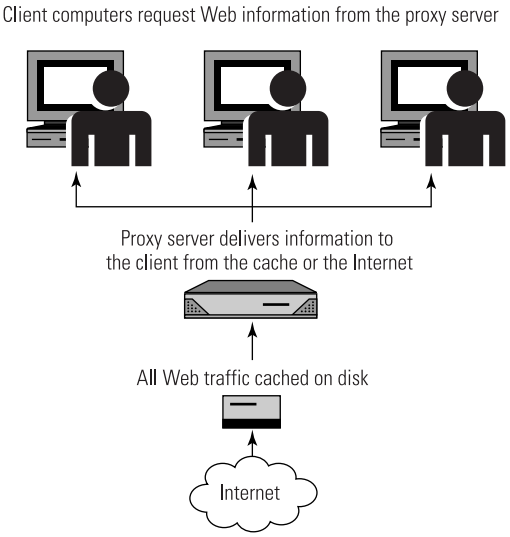
Proxy/Caching Feature

I-Gear is a proxy/cache server that runs on your Internet server. A proxy server is an application that acts as a gateway between your network and the rest of the Internet. If a client computer requests a document, the client computer asks the proxy server to retrieve the document instead of retrieving the document directly. Because I-Gear acts as the proxy between your network and the Internet, I-Gear is able to provide effective access control. The protocols proxied by I-Gear are Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS), and File Transfer Protocol (FTP).

I-Gear also has the ability to store on the server's hard disk the documents it downloads from the Internet. This storing process is known as caching. Network-based caching removes repetitive traffic from your Internet connection and can greatly enhance the performance of your communication line to the Internet. As shown in the figure below, when a user accesses information from a Web site, I-Gear stores that information on the server's hard disk as it forwards the information to the requesting user. The next time a user on the network requests data from this previously visited Web site, I-Gear verifies whether data stored on the hard disk are current by exchanging a few characters with the requested site and, if so, sends the previously stored information to the requesting user rather than tying up the communication line to the Internet to download the entire site again. If the information has changed, then I-Gear retrieves and stores the updated version.

For I-Gear to function properly, client computers must have the proxy settings of the Web browser configured to use I-Gear, or your network must be configured for transparent proxying. For information on config-

uring client workstations to use I-Gear, see the *I-Gear Installation Guide*.


Client computers request Web information from the proxy server
Proxy server delivers information to the client from the cache or the Internet
All Web traffic cached on disk
Internet

Note: If you are using I-Gear as a plug-in to either Check Point FireWall-1 or Microsoft Proxy Server and depending on your network and browser settings, the caching feature of I-Gear may not function. See the *I-Gear Installation Guide* for more information on using I-Gear as a plug-in.

I-Gear Objects

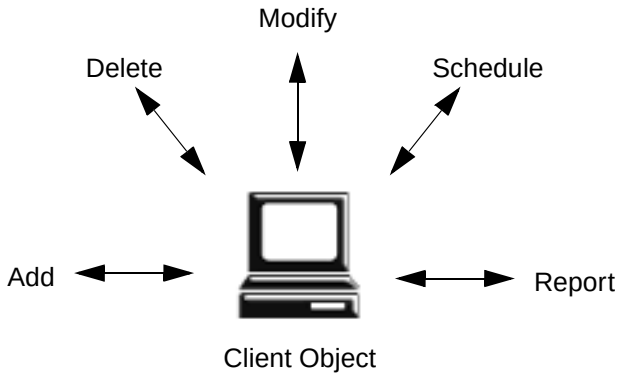
The I-Gear design philosophy is based on an object-oriented approach. Each network has users, client computers, and servers that are all part of the network. I-Gear classifies each of these entities as "objects" and uses intuitive methods for manipulating these objects. These objects are defined in the following table.

Object	Symbol	Description
Client		A Client is defined as a computer connected to the network with a unique IP address.
User		A User is defined as a person using your network. Users can be given unique permissions regardless of which computer on the network they use.

Object	Symbol	Description
Cast		A Cast is a group of Users or Clients that can be designated to operate in a specific manner. Casts can be scheduled to have different permissions, depending on the date and time of day. User and Client objects may belong to only one Cast.
List		A List object contains Uniform Resource Locators (URLs) that will be used to control access to certain sites. Lists can be uniquely applied to Client, User, Cast, or System objects by default or by date and time of day.
Dictionary		The DDR (Dynamic Document Review™) Dictionary contains words and phrases used to dynamically score pages as the material is downloaded. Based on this score, access to Web sites can be blocked or allowed. The DDR rules supplied by URLabs™ include context-sensitive information.
System		The System object is the actual server running I-Gear. The default properties for your network are established using the System object. The system can be set to automatically download new List objects from URLabs periodically if you have subscribed to this service.

I-Gear Methods

The I-Gear objects defined in the previous section are manipulated using methods. Methods are used to change the permissions or the functionality for each object. Five basic methods can be applied to I-Gear objects.



Not all methods are available for each object. For example, System objects cannot be added or deleted; thus, the Add and Delete methods

do not apply to the System object. The following table describes each method available in I-Gear and the objects toward which each method can be applied.

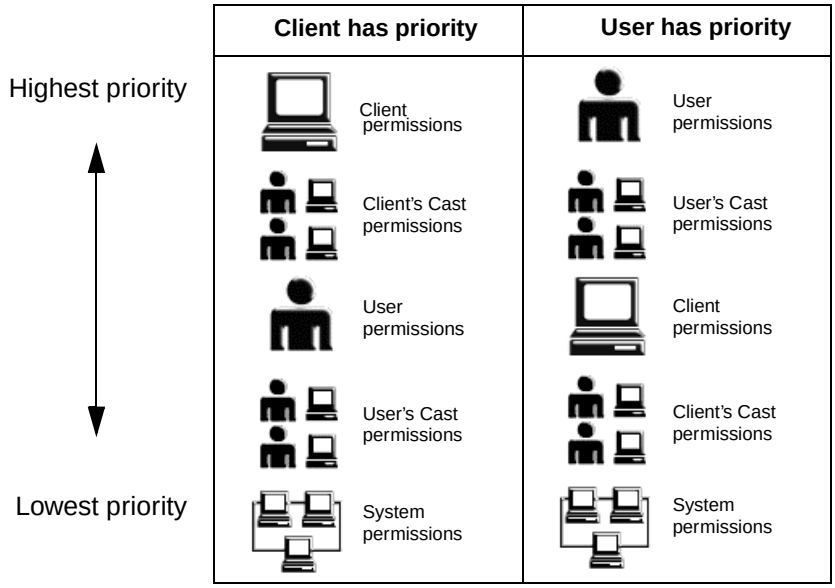
Method	Object	Description
Add	Client, User, Cast, List	The Add method is used to add I-Gear objects to the network.
Delete	Client, User, Cast, List	The Delete method is used to remove I-Gear objects from the network.
Modify	Client, User, Cast, List, Dictionary, System	The Modify method allows you to adjust the settings for defined objects. For example, URLs can be added to and deleted from Lists, and Cast memberships can be modified with the Modify method.
Schedule	Client, User, Cast, System	The Schedule method is used to define default access permissions, as well as to schedule access permissions based on date and time of day.
Report	Client, User, Cast, List, Dictionary, System	The Report method is used to show the activity for various objects. Reports can include, for example, Web sites that a Client, User, or Cast object has visited on the Internet or URLs that have been added to a List object.

Hierarchy of Permissions

In configuring I-Gear for your network, one concept that must be understood thoroughly is the priority that I-Gear assigns to different access permissions that have been set for I-Gear objects. For example, if a Client computer is locked (i.e., no Internet access is allowed from that machine) but a User who tries to use that computer has unfiltered and open access permissions, which permission has priority?

I-Gear's default settings specify that Client and Client Cast permissions take priority over User and User Cast permissions. You can reverse the hierarchy for object access permissions using the Modify method for the

System object. That is, you can specify that User and User Cast permissions take precedence over Client and Client Cast permissions.

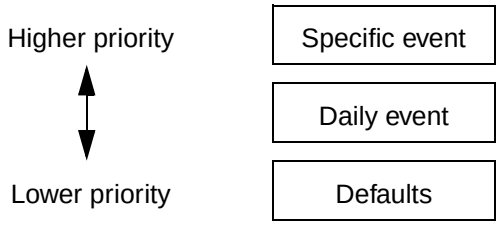


Thus, for the above example, whether or not the User could access the Internet from the given Client would depend on which object (User or Client) permissions were set to take precedence. If Client permissions had priority, the User, regardless of the assigned access permissions, would have no Internet access from the locked machine. If User permissions had priority, any User with access permissions would be able to browse from the Client, regardless of the Client settings.

Because you can schedule events for each object, the events for objects with the highest priority supersede the events and default permissions for the objects below them. For example, if a User's permissions are set to Locked (no Internet access permitted) and a Client Cast called "Room 141" is scheduled to have guest access with filtering turned on for machines in that room (and Client permissions have priority), then the User will have filtered Internet access in Room 141 and still be locked from other Clients not in that Cast.

Hierarchy of Events

In addition to the hierarchy of object permissions, types of events also have specific priorities, as shown below.



Specific events are scheduled for a specific date and time, such as October 27, 1998, from 2:00 PM to 3:00 PM. A specific event has the highest priority. After a specific event is past, it drops automatically from the system. Daily events reoccur each specified day, such as every Monday and Wednesday from 11:00 AM to 1:00 PM. You must delete a daily event (the event will continue to occur as specified until you cancel the event). Default settings apply when no other event is in effect.

Note: Objects, with the exception of the System object, are not required to have a default event. Clients, Users, and Casts inherit their default settings from the System defaults unless you specifically change the default settings for that object.

For example, you could schedule the computers in a school library to be locked by default. Then you could schedule a daily event that allows filtered Internet access on Monday through Thursday from 10:00 AM to 2:00 PM. You could then schedule a specific event on Monday, September 12, 1998, for a special faculty workshop with unfiltered Internet access from 11:00 AM to 1:00 PM. The specific event for Monday, September 12, would override the daily event that occurs every Monday.

3. Understanding Filter Lists and DDR

Filter lists are part of what I-Gear uses to control access to Internet sites. Predefined Content Category Lists are included with I-Gear. You can also create additional lists based on your specific needs.

Predefined Lists

A number of predefined Content Category Lists are included with I-Gear. URLabs has populated these lists with URLs that contain related subject matter. The following table describes each predefined list and includes sample URLs that are representative of the list content. (If you believe the URLs shown here are incorrectly categorized, please contact URLabs Support Services.)

List	Description
Crime	Sites providing instructions on performing criminal activities or acquiring illegal items, including defeating security, disabling, or otherwise interfering with computer systems (hacking or cracking); unauthorized use of telephone or communications equipment to place free calls or charge another's account for calls (phreaking); deactivating copy protection or registration schemes of software or hardware systems (pirating and warez); construction and usage of munitions such as pipe bombs, letter bombs, and land mines; and lock picking, spying, or general subterfuge and defeating of security measures. > http://www.2600.com/ > http://anarchistscookbook.com/
Drugs/Advocacy	Sites advocating the legal use of illegal drugs for medical and personal use. > http://www.mpp.org/ > http://www.norml.org/
Drugs/Nonmedical	Sites providing information on growth, distribution, and advocacy of drugs for nonmedical use (typically mood altering). Does not include alcohol or tobacco products. > http://www.cannabis.com/ > http://www.hightimes.com/
Entertainment/ Games	Sites dedicated to games, gaming, game tips, game downloads, interactive games, and multiplayer games. > http://www.wizards.com/ > http://www.gamesdomain.com/

List	Description
Entertainment/Sports	Sites dedicated to professional and amateur sports and sporting events. > http://cnnsi.com/ > http://www.espn.com/
Finance	Sites dedicated to personal finance, banking, stock trading, and wealth accumulation. > http://etrade.com/ > http://cnnfn.com/
Gambling	Sites dedicated to promotion of or participation in wagering, gambling, casinos, or lotteries. > http://www.valottery.com/ > http://www.virtualcasino.com/
Interactive/Chat	Sites providing interactive communication services, such as Webchat, bulletin boards, and IRC. > http://chat.yahoo.com/ > http://www.citylive.com/
Interactive/Mail	Sites providing interactive electronic-mail services. > http://www.hotmail.com/ > http://www.rocketmail.com/
Intolerance	Sites advocating intolerance or hatred of a person or group of people. > http://www.rahowa.com/ > http://www.k-k-k.com/
Job Search	Sites dedicated to job searching, job listings, resume exchanges, and head hunting. > http://www.jobsearch.com/ > http://www.monster.com/
News	Sites providing news coverage of regional and international events and weather services. > http://cnn.com/ > http://www.weather.com/
Sex/Acts	Sites depicting or implying sex acts, including pictures of masturbation not categorized under sexual education. Also includes sites selling sexual or adult products. > http://www.cyberos.com/ > http://persiankitty.com/

List	Description
Sex/Attire	Sites featuring pictures that include alluring or revealing attire, lingerie and swimsuit shopping, or supermodel photo collections but do not involve nudity. > http://www.victoriassecret.com/ > http://www.bikini.net/
Sex/Nudity	Sites featuring pictures of exposed breasts or genitalia that do not include or imply sex acts. Includes sites featuring nudity that is artistic in nature or intended to be artistic, including photograph galleries, paintings that may be displayed in museums, and other readily identifiable art forms. Includes nudist and naturist sites that contain pictures of nude individuals. > http://www.artcreate.com/photo/body/ > http://www.bareboating.com/
Sex/Personals	Sites dedicated to personals, dating, escort services, or mail-order marriages. > http://www.one-and-only.com/ > http://www.datingline.com/
SexEd/Advanced	Sites providing medical discussions of sexually transmitted diseases such as syphilis, gonorrhea, and HIV/AIDS. May include medical pictures of a graphic nature. Includes sites providing information of an educational nature on pregnancy and family planning, including abortion and adoption issues. Also includes sites providing information on sexual assault, including support sites for victims of rape, child molestation, and sexual abuse. Includes sites providing information and instructions on the use of birth control devices. May include some explicit pictures or illustrations intended for instructional purposes only. May include slang names for reproductive organs or clinical discussions of reproduction. > http://www.plannedparenthood.org/ > http://www.immunet.org/
SexEd/Basic	Sites providing information at the elementary level about puberty and reproduction. Includes clinical names for reproductive organs (e.g., penis). > http://contraception.net/ > http://www.mum.org/

List	Description
SexEd/Sexuality	Sites dealing with topics in human sexuality. Includes sexual technique, sexual orientation, cross-dressing, transvestites, transgenders, multiple-partner relationships, and other related issues. > http://www.youth.org/ > http://www.inetnorth.ab.ca/users/CherylBB/
Violence	Sites depicting or advocating violence, including sites promoting violent terrorist acts against others that do not fall under the “Intolerance” category. > http://www.usapublications.com/ > http://www.shotgunvideo.com/
Weapons	Sites that display, sell, or advocate the use of weapons, including guns, knives, and martial-arts weaponry. > http://www.nra.org/ > http://www.shooters.com/
allow	Historical default list for sites to which access is to be permitted. This list is empty when I-Gear is initially installed.
deny	Historical default list of sites to which access is to be denied. This list is empty when I-Gear is initially installed.

Two versions of each predefined Content Category List exist in I-Gear: a local version and the version populated by URLabs. The local version of each list is provided so that you can add additional URLs to various lists as necessary.

Note: When a request for Internet access is made, I-Gear checks the local versions of all active lists before it checks the URLabs versions; if I-Gear finds a match in one or more active local lists (i.e., lists not in the Off state), it will NOT check the URLabs versions of the lists. Thus, you can completely override any URLabs categorization of a site if you wish by adding the site to a local list, and you can add additional sites not contained in the URLabs-provided lists.

The predefined Content Category Lists are continually updated by URLabs. I-Gear will automatically download updated Lists periodically if you have subscribed to the List updates. These updates release you from trying to identify all sites on the Internet that fall within the content categories. If you do not subscribe to the List updates, then you will need to update your local Lists frequently to keep pace, as new sites are continually brought online.

Note: New predefined Content Category Lists will periodically be created by URLabs as necessary to address additional content areas. If you subscribe to the List updates, these new Lists will automatically be downloaded along with the regular updates to existing Lists. New Lists will be in the Off state and will need to be activated as appropriate.

Local Lists

You can also create any number of your own Lists. You may want to create specific Lists of sites you have identified for a specific use. For example, you may want to create a List containing sites with information on earthquakes and allow students access to only that List for a specific project.

List States

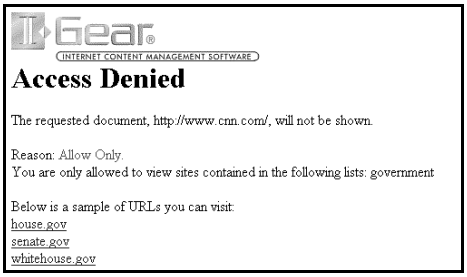
Each List is in one of four states—Allow (Filtering Enabled), Allow (Filtering Disabled), Deny, or Off. The state of each List is set when scheduling objects. Thus, the state of each List can be different based on the access restrictions for individual Users, Clients, or Casts.

State	Description
Allow (Filtering Enabled)	Requests for URLs contained in an Allow (Filtering Enabled) List are permitted, and the document text is scanned by DDR.
Allow (Filtering Disabled)	Requests for URLs contained in an Allow (Filtering Disabled) List are permitted, and the document text is not scanned by DDR.
Deny	Requests for URLs contained in a Deny List are not permitted. When a request is made for a URL contained in a Deny List, an I-Gear "Access Denied" page is displayed to the requesting User, indicating the List in which the URL was found.
Off	Lists in the Off state are not consulted when I-Gear is checking Lists for URLs. Thus, requests for URLs contained in an Off List are not denied, and the document text is subject to DDR review.

Allow Lists

Allow Lists should usually contain URLs known to contain material appropriate for a particular activity. You can choose either Allow (Filtering Enabled) or Allow (Filtering Disabled). Keep in mind that setting a List to Allow (Filtering Disabled) allows unconditional access to the URLs in that List. Allow Lists often are used to restrict Users or Clients

to accessing only permitted URLs. Objects (i.e., Users, Clients, or Casts) scheduled for Allow Lists Only access can view only URLs in Lists in either of the Allow states; thus, when a request is made for a URL not in the assigned Lists, the request is blocked, and an I-Gear "Access Denied" page that lists the permitted URLs is returned.


I-Gear
INTERNET CONTENT MANAGEMENT SOFTWARE
Access Denied
The requested document, http://www.cnn.com/, will not be shown.
Reason: Allow Only.
You are only allowed to view sites contained in the following lists: government
Below is a sample of URLs you can visit:
house.gov
senate.gov
whitehouse.gov

Note: Allow Lists are overridden by Deny Lists. Thus, even if you place a URL in an Allow List, if that URL appears in any List currently in the Deny state, the URL still will be blocked.

Deny Lists

A Deny List usually contains URLs known to contain inappropriate material. Deny Lists override Allow Lists. Thus, if you place the same URL in two different local Lists—for example, Sex/Acts and Sex/Nudity—and the Sex/Acts List is in the Deny state and the Sex/Nudity List is in the Allow state for a given User, access to the site still will be denied because at least one List in the Deny state contains the site.

Objects (i.e., Users, Clients, or Casts) scheduled for Filtered Access are prevented from accessing URLs in the assigned Deny Lists. When a request is made for a URL in an assigned Deny List, the request is blocked, and an I-Gear "Access Denied" page is returned to indicate the list in which the denied URL was found.

I-Gear
INTERNET CONTENT MANAGEMENT SOFTWARE
Access Denied
The requested document, http://www.rahowa.com/, will not be shown.
Reason: Found in Denied List (Intolerance).

Off Lists

The Off state is used to cancel the effect of a List. Lists in the Off state are not consulted. The URLs contained in an Off List are not denied and are still subject to screening by DDR.

Note: When I-Gear is initially installed, the predefined Lists are in the Off state. Most sites will want to immediately change after installation the state of some of these Lists to Deny, based on local acceptable-use policies. Step-by-step instructions for initially configuring this aspect of I-Gear are included in the *I-Gear Installation Guide*.

Note: Two predefined Lists (i.e., "allow" and "deny") have names that, for historical reasons, indicate state. The Lists are intended to be used as the names imply (i.e., the allow List is meant to be in the Allow state). However, you can put the "allow" List in the Deny state and the "deny" List in the Allow state if you so choose.

Adding URLs to Lists

I-Gear looks for the most exact match when checking a URL against assigned Lists. Thus, you can block or allow individual Web pages or entire directories, machines, or domains.

Filtered URL	Effect
`www.badsite.com/pics/apr.html`	Matches this one specific page.
`www.badsite.com/pics`	Matches entire directory.
`www.badsite.com`	Matches this machine.
`badsite.com`	Matches entire domain.

For example, if your Deny List contained `badsite.com`, access to all URLs in that domain would be denied. However, suppose a site within that domain contained some content to which you wanted to permit access. You could add to an Allow List the specific directory that contained the desirable content (e.g., `www.badsite.com/daily-news`). Thus, because I-Gear looks for the most exact match, access to that directory would be permitted, while access to any other content from that domain would still be denied.

Note: I-Gear for FireWall-1 has access to only actual IP addresses rather than to the domain names used in the figure above; thus, domain check-

ing is not effective with FireWall-1. (However, I-Gear still searches for the most exact match.) Thus, with FireWall-1, when you enter a URL in a local List, I-Gear attempts to identify all IP addresses associated with that URL. However, this list of IP addresses may not be complete and is subject to periodic change. Periodic review and update of the IP addresses contained in your local Lists are necessary in maintaining local Lists. The URLabs versions of all predefined Content Category Lists are kept up to date. If you subscribe to List updates, you will automatically receive any changes of this type with your regular List updates.

Dynamic Document Review

A powerful feature of I-Gear is its ability to review the content of a site as the information is being downloaded to the User. Because of the Internet's size and the variety of sites, creating and maintaining Lists of all sites that potentially contain objectionable material would be impossible. The robust capabilities of today's search engines and Web robots enable users to find sites not in Deny Lists. Furthermore, the language returned by search engines in the descriptions of sites may be objectionable to some people even if the actual site is contained in a Deny List. I-Gear scans each page and header to perform a real-time evaluation of the information. This process is referred to as Dynamic Document Review (DDR).

When a User requests a URL from the Internet, I-Gear first matches the URL against the Lists, as discussed previously. If the URL is not found in any assigned Allow or Deny Lists, I-Gear further processes the document's content to determine its suitability. For example, if a User clicks on a site such as `www.badsite.com` and that site is not contained in any of the assigned Deny or Allow Lists, I-Gear scans the headers and contents of the page as it is retrieved from the Internet.

To determine whether access to a site should be blocked or allowed, I-Gear matches the text from the requested site against predefined DDR Dictionaries that contain potential trigger words, in several languages. Each occurrence of a word contained in an active Dictionary receives a numerical score, and I-Gear keeps a total score for a given amount of text. If the total score exceeds 50 (a score of 50 is the default setting),

I-Gear blocks access to the site and sends an “Access Denied” message to the requesting User’s Web browser.

If a page is blocked by DDR, the resulting score is shown.

Note: If objectionable words are found on a page as the information is being retrieved and scanned, I-Gear automatically replaces the objectionable words in the text. For example, “`badword`” would be replaced with “`----`” in the text, even in the site description returned to the User by the search engine.

Note: Each of I-Gear’s predefined Lists has an associated DDR Dictionary with trigger words that has been populated by URLabs. When a particular List is placed in either of the Allow states (Filtering Disabled or Filtering Enabled) or in the Off state, I-Gear assumes that the type of content associated with that List is acceptable and does not use the Dictionary associated with that List in DDR scanning.

I-Gear allows you to change the sensitivity of DDR. The default setting is a score of 50. Thus, at the default setting, any page that receives a score of 50 or above will be blocked. You can adjust DDR to be more or less restrictive by selecting another score choice in a range of 1 to 200.

In addition to unconditionally vulgar words, I-Gear also looks for words that are conditionally inappropriate. I-Gear reviews each word on a page and examines the surrounding words to determine the context of conditionally inappropriate terms. For example, in a standard filtering configuration the following two phrases are rated differently by DDR.

Phrase	Action
`Hot sexual pictures`	DDR rates this string of words with a positive score.
`Sexual harassment`	DDR rates this string of words with a score of zero (no effect).

A local version of each Dictionary is also provided. You can add words to any or all of these Dictionaries based on your specific requirements. When you enter a word in a local Dictionary, you must also provide a point value for the word for use in DDR scoring. Local Dictionary

entries override predefined Dictionary entries for the same word. Thus, if you add the word “sex” to the Sex/Acts Dictionary, with a score of 5 points for that word, and that word already exists in the predefined Dictionary with a different point value, your point value is the one DDR will use in scoring Web sites.

Note: Try not to be overly aggressive in adding what may be considered “conditionally objectionable” words to the DDR Dictionary. Entering words such as “sex” or “bottom” will likely cause many more pages to be blocked than you may intend. Keep in mind that the default settings, predefined Dictionaries, and predefined Lists included in I-Gear have been designed to filter Internet content effectively. Initially, simply adjusting the sensitivity of DDR to suit your local policies rather than adding a large number of words to Dictionaries may be more effective in achieving the desired level of filtering. Then as you become familiar with I-Gear’s functionality, you can add additional words to Dictionaries as needed.

A Web page is scored in sections as the page is being retrieved (rather than scored by entire page). This feature allows Users with filtered access on your network to view a page that is not objectionable at the beginning but blocks access to later sections of the page if these sections are rated as objectionable.

The context review performed by DDR is based on extensive rules supplied with the I-Gear package. These rules, along with the categorized filter Lists, are routinely updated and refined. I-Gear will automatically download updated Lists and rules periodically if you have subscribed to the List updates.

How Filter Lists and DDR Work Together

This section is intended to clarify the use of filter Lists and DDR to achieve desired degrees of filtering. Examples are included in this section to demonstrate the steps that I-Gear follows in filtering when a request for Internet access is made.

The unique filtering capability of I-Gear is a result of the combined effectiveness of the Content Category Lists and DDR. You control the degree of filtering applied to objects by placing Lists in one of four states discussed earlier. Depending on the state of a particular List, access to the URLs contained in the List may be restricted or allowed, and the corresponding Dictionary may or may not be used by DDR to score Web-page content. Thus, by placing Lists in different states, you

control not only access to sites contained in Lists but whether DDR is filtering for a particular type of content. The following reference table shows the relationship of the Content Category Lists and the corresponding Dictionaries and how each one functions based on the state in which a Content Category List is placed.

Note: In the following table, the Sex/Acts List is used only as an example. The predefined Content Category Lists are generally NOT intended to be in either of the Allow states (Filtering Enabled or Filtering Disabled) for the System default settings. Based on your local acceptable-use policies, you will probably want to place some of the predefined Lists in the Deny state (to restrict access to all URLs in that list) and leave some Lists in the Off state (to cancel the effect of the List and permit access to the contained URLs). Placing the predefined Content Category Lists in either of the Allow states is not recommended.

		LIST (for example, Sex/Acts)		CORRESPONDING DICTIONARY (Sex/Acts)	
		PREDEFINED VERSION: contains URLs added by URLabs; updated daily with subscription	**LOCAL VERSION:** contains additional URLs added locally as necessary	**PREDEFINED VERSION:** contains words and point values provided by URLabs for DDR scoring	**LOCAL VERSION:** contains additional words and point values added locally as necessary
ALLOW (Filtering enabled)	What happens when you place Sex/Acts list in the **Allow (Filtering Enabled)** state?	✓ Access to URLs in Sex/Acts list not denied ✓ DDR scans content of URLs (using ONLY activated Dictionaries for scoring)		✓ Terms and point values in Sex/Acts Dictionary NOT used by DDR in scoring	
ALLOW (Filtering disabled)	What happens when you place Sex/Acts list in the **Allow(Filtering Disabled)** state?	✓ Access to URLs in Sex/Acts list permitted ✓ DDR does NOT check URLs		✓ Terms and point values in Sex/Acts Dictionary NOT used by DDR in scoring	
DENY	What happens when you place the Sex/Acts list in the **Deny** state?	✓ Access to URLs in Sex/Acts list NOT permitted		✓ Terms and point values in Sex/Acts Dictionary used by DDR in scoring	
OFF	What happens when you place the Sex/Acts list in the **Off** state?	✓ Access to URLs in Sex/Acts list not denied ✓ DDR scans content of URLs (using ONLY activated Dictionaries for scoring; note that Sex/Acts Dictionary is NOT activated)		✓ Terms and point values in Sex/Acts Dictionary NOT used by DDR in scoring	

The table above demonstrates how I-Gear applies filtering according to List states. In managing your Lists, determine the appropriate List states to be used for certain types of information. Use the following table as

general guidance on recommended states for particular types of List content.

List state	List content
Allow (Filtering Enabled)	Lists containing sites to which you want to generally allow access or to which you would not want to block wholesale access, but for which you do not have complete confidence that the content will remain acceptable (e.g., search engines, such as `www.altavista.com`, knowing that DDR will still block access to any objectionable or inappropriate content as necessary).
Allow (Filtering Disabled)	Lists containing sites to which you want to allow access and for which you have confidence that the content will remain acceptable (e.g., `www.disney.com`).
Deny	Lists containing sites to which you definitely do not want to allow access (e.g., `www.penthouse.com`).
Off	Predefined Content Category Lists you do not want to be filtered (e.g., the predefined List Interactive/Chat could be placed in the Off state given acceptable-use policies that considered chat to be generally acceptable, keeping in mind that DDR will still block certain chat topics based on other filtering that might be in effect).

The following examples illustrate in detail each step in the process that I-Gear uses to determine whether to allow or deny access to a site requested by a given User. The table details each decision point reached by I-Gear, subject to filtering currently in effect, in determining whether to allow or deny access to a site. In each example, User `jsmith` requests access to a particular site. The basic filtering that applies to the User is given for each example.

Example 1: The User requests access to the site `www.pornography4U.com`. User `jsmith` is in Filtered mode, and the URLabs predefined Content Category Lists Sex/Acts and Sex/Nudity are in the Deny state for this User; thus, material of this type is considered objectionable for this User. However, the requested site is a new Internet site and has not yet been published in a Content Category List by URLabs and does not appear in any local lists on your network.

Example 2: User `jsmith` is in Allow Only mode for a period of focused research on government. He has accessed the House of Repre-

sentatives home page, www.house.gov, which has been placed in a local Allow (Filtering Enabled) list called "government" for this research period. While searching this site, he comes across the Independent Counsel Kenneth Starr's Report to the U.S. House of Representatives.

Example 3: User jsmith is enrolled in an art class focusing on the human body as an art form. The teacher has identified several sites she wants to allow the art students to access. These sites contain some nude photography and are contained in the predefined Sex/Nudity Content Category List. She does not want to allow access to the entire Sex/Nudity List, but she wants to override for the semester the filtering on these few sites. She places the URLs for these sites into a new local List called Art, and she places the List in the Allow (Filtering Disabled) state for the students in the art class. The students, including jsmith, remain in filtered mode, with the Sex/Nudity and Sex/Acts Lists in the Deny state and the Art List in the Allow (Filtering Disabled) state. In this example, User jsmith requests one of the sites contained in the Art List: www.drawingthehumanbody.com.

I-Gear's action	Result
Step 1: First, I-Gear checks the local versions of all Lists for the requested URL.	If the URL is found in any local List, I-Gear allows or restricts access based on the state of the List. If the URL is contained in more than one local List and the Lists are in different states, I-Gear uses the following hierarchy in terms of states: Deny, Allow (Filtering Enabled), and then Allow (Filtering Disabled). Thus, if the URL is contained in any local List in the Deny state, access to the site will be denied, even if the URL is also contained in any local List(s) in either of the Allow states. If the URL is found in any local List, I-Gear does NOT check the predefined Lists published by URLabs. **Example 1:** In this example, the requested site, www.pornography4U.com, is not found in any local List; thus, I-Gear goes to the next step. **Example 2:** In this example, the User, in Allow Only mode, is allowed to initially access the site www.house.gov because this site is contained in the local List entitled "government" in the Allow (Filtering Enabled) state. Because the List is in the Allow (Filtering Enabled) state, DDR (using all active Dictionaries) is still running on any URL accessed by the User.

I-Gear's action	Result
	Example 3: In this example, I-Gear finds the requested URL, `www.drawingthehumanbody.com`, in only one local List, Art, which is in the Allow (Filtering Disabled) state. Thus, User `jsmith` is allowed access to this site.
Step 2: If the URL is not found in ANY local List, then I-Gear checks the predefined Lists populated by URLabs for the requested URL.	If the URL is found in any predefined List, I-Gear allows or restricts access based on the state of the List. If the URL is contained in more than one predefined List and those Lists are in different states, I-Gear will use the following hierarchy in terms of state: Deny, Allow (Filtering Enabled), and Allow (Filtering Disabled). Thus, if the URL is contained in any predefined List in the Deny state, access to the site will be denied, even if the URL is also contained in any predefined List(s) in either of the Allow states. **Example 1:** In this example, the requested site, `www.pornography4U.com`, is not found in any predefined List. The site is new, and URLabs has not published the site in any Content Category List yet; thus, I-Gear goes to the next step. **Example 2:** I-Gear does not check the predefined Lists for `www.house.gov` because the URL is contained in a local List. **Example 3:** I-Gear does not check the predefined Lists for `www.drawingthehumanbody.com` because the URL is contained in a local List.
Step 3: For any document that has not been denied as a result of being contained in a List in the Deny state, I-Gear applies DDR to the document content (UNLESS that URL is contained in a List in the Allow (Filtering Disabled) state). DDR runs on small blocks of text as the information is being downloaded from the Internet.	DDR uses the active Dictionaries (i.e., Dictionaries for any Lists in the Deny or Allow (Filtering Enabled) states) to score the content of the Web site as the document is being downloaded from the Internet. If the score for any block of text reaches the DDR threshold established for the requesting User, I-Gear blocks access to the site. **Example 1:** In this example, because the Sex/Nudity and Sex/Acts Dictionaries are in the Deny state for the requesting User, the DDR score is well over the DDR threshold established for this User. Thus, I-Gear blocks the User's access to the requested site, `www.pornography4U.com`.

I-Gear's action	Result
	Example 2: In this example, DDR continues to scan the new information as it is downloaded for User `jsmith` from the domain `www.house.gov`. The User is allowed to access the requested material until the DDR threshold for a given block of material exceeds that established for the User. Thus, when User `jsmith` gets to the portion of the Starr Report that contains objectionable content, DDR blocks the remainder of the document from being shown.
	Example 3: In this example, DDR does not run on the requested URL because the URL is contained in a List in the Allow (Filtering Disabled) state. Thus, the User is not blocked from accessing this site for any reason.

4. I-Gear User Interface

The I-Gear User interface is ideally suited for large Internet-based networks in which Users do not have dedicated computers or where Client computers do not require User authentication. With the I-Gear interface, Users can use a Web browser on an Apple® Macintosh® computer at one location and later move to a Microsoft Windows® 95-based computer at another location and still retain their bookmarks and previously visited sites (history).

The I-Gear User interface is designed to allow easy access to the I-Gear functions. To use this interface, you will need a Web browser that supports frames and, optionally, JavaScript 1.1. Netscape Navigator® 2.0 or later and Microsoft Internet Explorer 3.0 or later are two examples of Web browsers. The I-Gear User interface

- Optionally requires Users to log in to access the Web, regardless of the type of computer they are using.
- Provides bookmarks that travel with the User on the network.
- Provides quick access to the administrative functions of I-Gear (permissions permitting).

The I-Gear Tool Bar

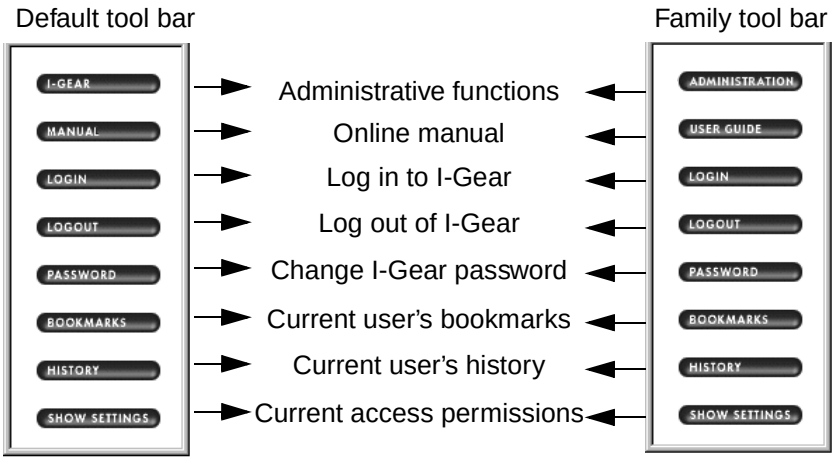
The I-Gear tool bar consists of a series of buttons that are hypertext links to the various functions of the I-Gear suite. These buttons vary slightly depending on the administrative interface that is being used (Enterprise version only). To invoke the I-Gear tool bar, visit the URL

`http://<servername>:port/toolbar`

where *<servername>* is the host name or IP address of the server running I-Gear. I-Gear provides a Web server for its own use; this server is assigned a port number (8002 is the default). Thus, all accesses to the I-Gear administrative and User interfaces begin with `http://<servername>:port/`.

The tool bar will also activate whenever a login screen is displayed (if JavaScript is enabled on your browser). I-Gear will allow you to define a home page to display in the main browser window after a User logs in to I-Gear. This default home page will appear with the I-Gear tool bar.

The figure below shows the functionality of each button on the tool bar. The **I-Gear/Administration, Manual/User Guide,** and **Password** buttons appear only if the current User has been granted permissions related to that particular function. For example, a User who does not have permission to change their password will not see the **Password** button.



The I-Gear tool bar can appear in two forms, depending on the type of browser and the browser's capabilities. If your browser supports JavaScript 1.1, the I-Gear tool bar will appear in a separate window. This tool bar will remain in a separate window regardless of the URLs visited in the main browser window. If your browser does not support JavaScript or if JavaScript is turned off, the tool bar will appear in a side frame within a single browser window.

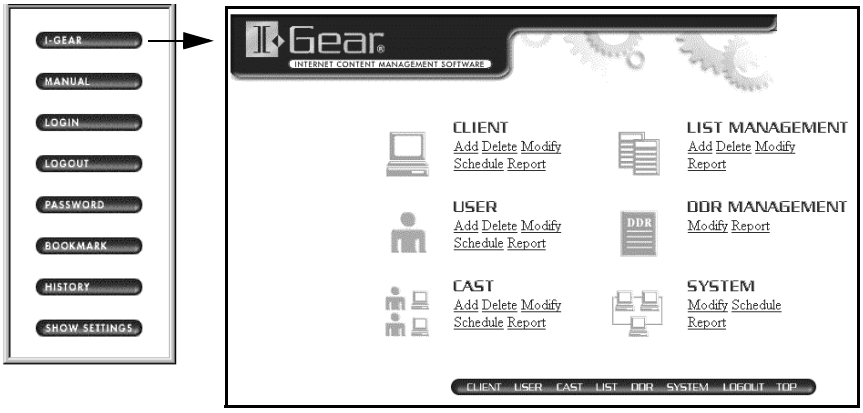
Accessing Administrative Functions

Users with administrative permissions can access I-Gear's administrative interface through the I-Gear tool bar.

```
http://<servername>:port/admin
```

Note: If you are using the Enterprise version of I-Gear, two administrative interfaces are available: the standard interface and the family interface. The interface that is displayed for a given User depends on the settings that may have been established for the User and the Client that is being used.

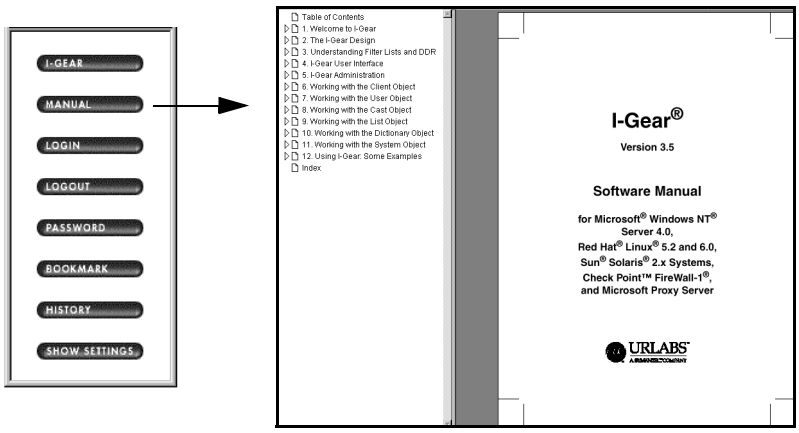
Click the **I-Gear** button (or the **Administration** button if you are using the family interface), and the appropriate I-Gear administrative interface will be displayed.



You can also visit the following URL to access the administrative interface.

Accessing Online Manuals

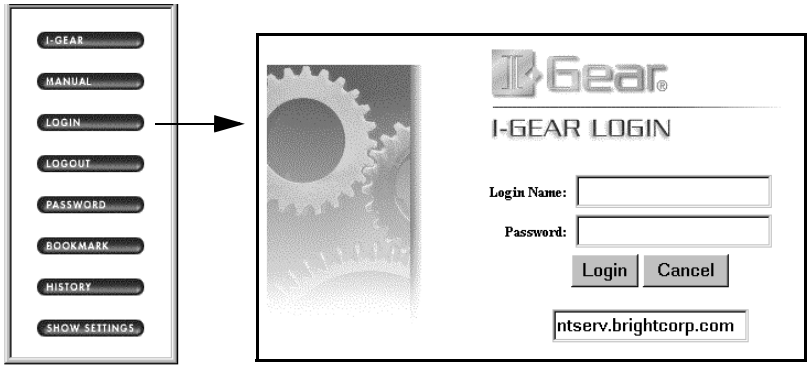
Users with administrative permissions can also access the *I-Gear Software Manual* or the *I-Gear User Guide* in .pdf format, depending on the administrative interface that is being used. Click the **Manual** button (or the **User Guide** button if you are using the family interface), to display the manual and the table of contents in the browser window.



Logging In

If a User attempts to use a Client for which login is required, a login screen will appear when the User tries to visit an Internet site outside the local network. The login feature can be disabled, as outlined in later this manual. If a Client does not require Users to log in but certain Users want to access their portable bookmarks and history, Users will be prompted after clicking the **Bookmark** or **History** button to provide their login name and password before their personal history and bookmarks will be displayed.

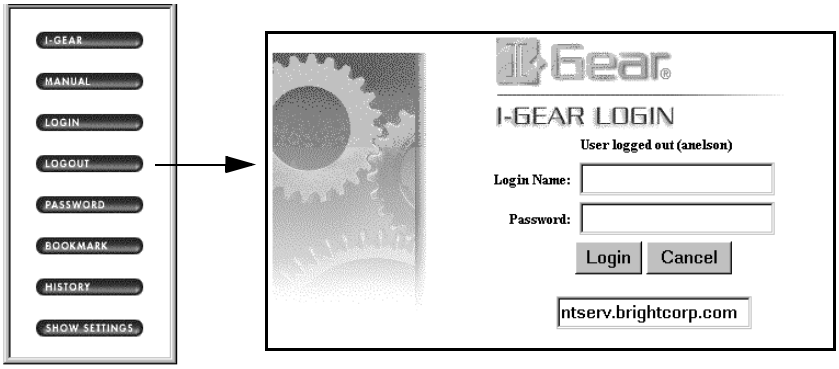
Note: If you are using I-Gear for MS Proxy and have selected the Get Login Information from MS Proxy option, Users may not be prompted with the I-Gear login screen after launching the Web browser. The browser instead will immediately display the default URL. Depending on the browser used, however, Users may be prompted at times with an authentication window in which they will need to provide login name and password. For information on activating the Get Login Information from MS Proxy option, see page 58. (Note that access to an I-Gear administrative interface requires a User to log in to I-Gear regardless of whether this option has been activated.)



Logging Out

To log out of I-Gear, click the **Logout** button located on the I-Gear tool bar. After a User has logged out, access to off-site Internet sites or to the

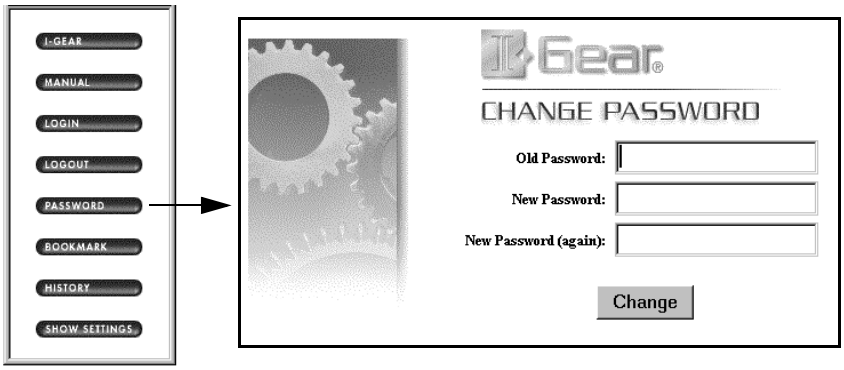
administrative functions will not be permitted from the machine until a User begins a new session by logging in.



Note: Quitting the Web browser alone is not sufficient to log out of I-Gear. (However, quitting the Web browser is sufficient to eliminate access to any administrative functions held by the previous User.) A User must click the **Logout** button to prevent the next User from being able to browse (on the same machine) using the previously logged-in User's account. If a Client has no activity for a given period of time (5 minutes is the default time period), the current User is automatically logged out of I-Gear.

Changing a Password

Users who have been granted permission to change their own password can do so by clicking the **Password** button on the tool bar. This button will not display on the tool bar for Users who have not been given password permission. First enter your current password in the appropriate field. Then enter your new password in the fields provided so that I-Gear can verify the new password. Then click the **Change** button.



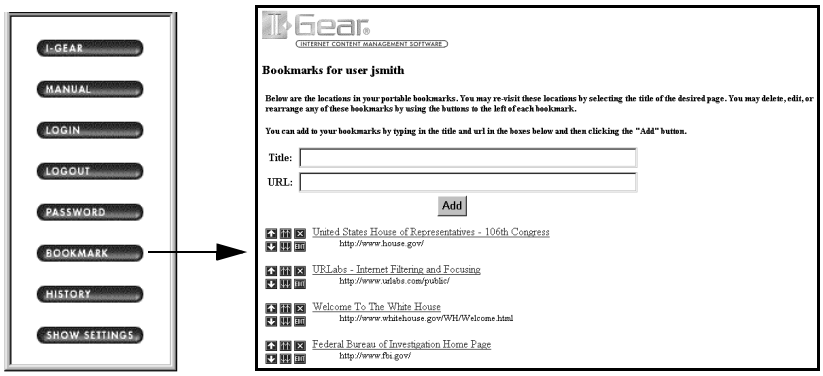
Note: Check with your site administrator for any local password policies or conventions.

Accessing Bookmarks and History

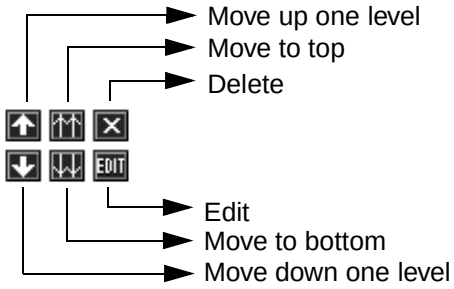
I-Gear allows Users to access their bookmarks and their access history regardless of the location or the type of computer used on the network. To access your I-Gear bookmarks, click the **Bookmark** button on the tool bar. Bookmarks are displayed as shown below; the title for each bookmark is an active link.

Note: You must be logged in to access your bookmarks and history. If you click the **Bookmark** or the **History** button and you have not logged in, I-Gear will prompt you with the login screen before displaying your bookmarks or personal history.

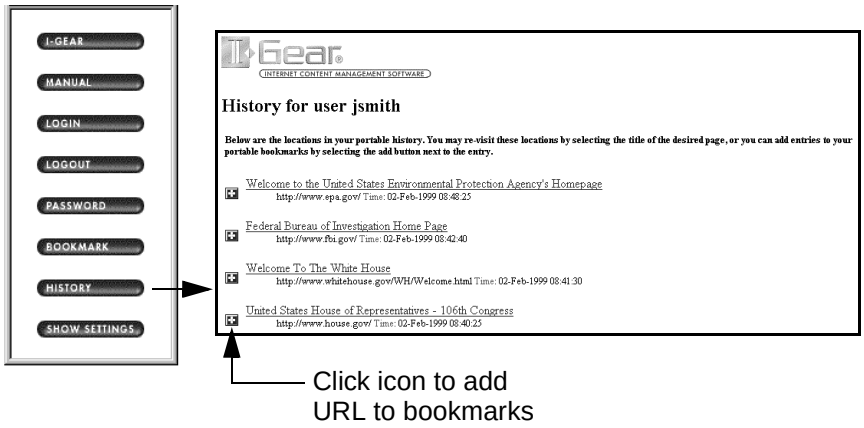
You can manually add new bookmarks using the fields provided. (You can also add bookmarks automatically from your history.) Enter the title in the appropriate field for the site you wish to add. (The title entered in this field will be the title under which the site is listed, so you should use a sufficiently descriptive title.) Then enter in the appropriate field the entire URL for the site, and click the **Add** button.


I-GEAR
MANUAL
LOGIN
LOGOUT
PASSWORD
BOOKMARK
HISTORY
SHOW SETTINGS
Gear
INTERNET CONTENT MANAGEMENT SOFTWARE
Bookmarks for user jsmith
Below are the locations in your portable bookmarks. You may re-visit these locations by selecting the title of the desired page. You may delete, edit, or rearrange any of these bookmarks by using the buttons to the left of each bookmark.
You can add to your bookmarks by typing in the title and url in the boxes below and then clicking the "Add" button.
Title:
URL:
Add
United States House of Representatives - 106th Congress
http://www.house.gov/
URLabs - Internet Filtering and Focusing
http://www.urlabs.com/public/
Welcome To The White House
http://www.whitehouse.gov/WH/Welcome.html
Federal Bureau of Investigation Home Page
http://www.fbi.gov/

The buttons associated with each bookmark allow you to move the bookmark up or down within the bookmark list, as well as to edit or delete the bookmark.



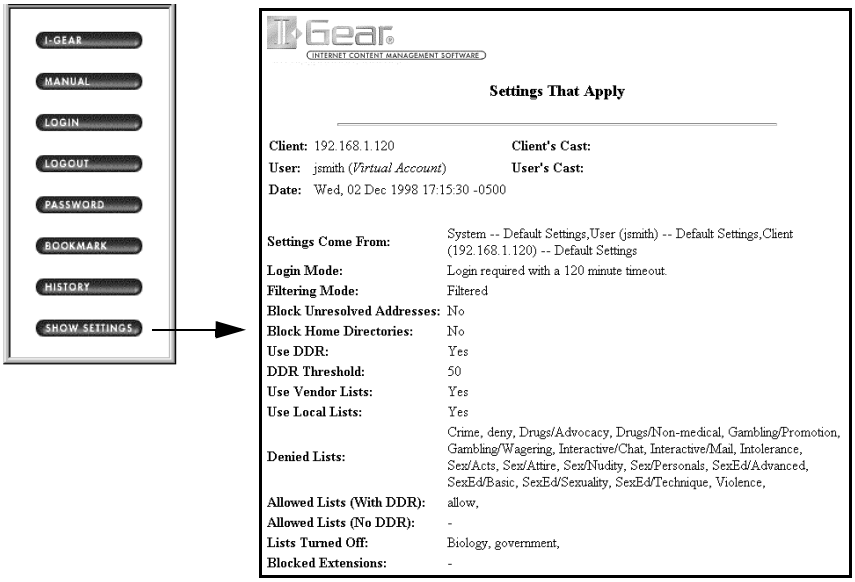
In addition to the bookmark feature, I-Gear maintains a recent history of sites visited by a given User. Click the **History** button to display the 20 most recently visited sites. You can quickly add to your bookmarks any sites displayed in your history by clicking the **Add** icon next to the selected site.


I-GEAR
MANUAL
LOGIN
LOGOUT
PASSWORD
BOOKMARK
HISTORY
SHOW SETTINGS
I-Gear
INTERNET CONTENT MANAGEMENT SOFTWARE
History for user jsmith
Below are the locations in your portable history. You may re-visit these locations by selecting the title of the desired page, or you can add entries to your portable bookmarks by selecting the add button next to the entry.
Welcome to the United States Environmental Protection Agency's Homepage
http://www.epa.gov/ Time: 02-Feb-1999 08:48:25
Federal Bureau of Investigation Home Page
http://www.fbi.gov/ Time: 02-Feb-1999 08:42:40
Welcome To The White House
http://www.whitehouse.gov/WH/Welcome.html Time: 02-Feb-1999 08:41:30
United States House of Representatives - 106th Congress
http://www.house.gov/ Time: 02-Feb-1999 08:40:25
Click icon to add
URL to bookmarks

Showing Filter Settings

The access permissions for the current User and Client can be viewed by clicking the **Show Settings** button on the tool bar. This function can be helpful in determining why a particular User or Client cannot access a given URL. The display indicates, based on the I-Gear permission hierarchy (i.e., Client, User, Cast, and System), those permissions that are applicable to the current User and Client. The **Show Settings** display indicates, for example, how filtering is being applied and indicates the states of all Lists as they apply to that User and Client (i.e., whether the

Lists are in the Allow (Filtering Enabled), Allow (Filtering Disabled), Deny, or Off state).


I-GEAR
MANUAL
LOGIN
LOGOUT
PASSWORD
BOOKMARK
HISTORY
SHOW SETTINGS
Gear
INTERNET CONTENT MANAGEMENT SOFTWARE
Settings That Apply
Client: 192.168.1.120
Client's Cast:
User: jsmith (Virtual Account)
User's Cast:
Date: Wed, 02 Dec 1998 17:15:30 -0500
Settings Come From: System -- Default Settings,User (jsmith) -- Default Settings,Client (192.168.1.120) -- Default Settings
Login Mode: Login required with a 120 minute timeout.
Filtering Mode: Filtered
Block Unresolved Addresses: No
Block Home Directories: No
Use DDR: Yes
DDR Threshold: 50
Use Vendor Lists: Yes
Use Local Lists: Yes
Denied Lists: Crime, deny, Drugs/Advocacy, Drugs/Non-medical, Gambling/Promotion, Gambling/Wagering, Interactive/Chat, Interactive/Mail, Intolerance, Sex/Acts, Sex/Attire, Sex/Nudity, Sex/Personals, SexEd/Advanced, SexEd/Basic, SexEd/Sexuality, SexEd/Technique, Violence,
Allowed Lists (With DDR): allow,
Allowed Lists (No DDR): -
Lists Turned Off: Biology, government,
Blocked Extensions: -

Showing Filter Settings for Other Users

Normally, clicking the **Show Settings** button shows the applicable filtering settings for the User that is currently logged in and the current Client workstation. However, if the logged-in User has Reporting permission for the System object, that User can view the settings for another User simply by adding the appropriate User name to the Show Settings URL. This feature allows an administrator to check filtering settings for any User regardless of the administrator's location relative to the User.

The URL for the Show Settings display normally appears as follows for the logged-in User:

`http://<servername>:port/showsettings`

If you change the URL by adding the string `?user=<username>`, where `<username>` is the User whose settings you want to display, so that the URL reads as

`http://<servername>:port/showsettings?user=<username>`

then the settings for the specified User will be displayed.

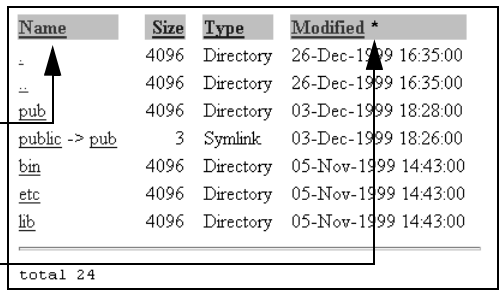
Sorting Feature for FTP

If you are using I-Gear to proxy FTP requests, I-Gear can conveniently organize data at an FTP site in several ways: alphbetical by name, by the size of the directory or file, according to type, or by date last modified. This sort feature can be helpful in locating certain files or directories on larger sites.

In the browser display for an FTP site, column headings are actually links. Click the link at the top of the Name, Size, Type, or Modified column to sort the entries according to the criteria for that column. A single click on a header should sort the messages in descending order according to the criteria for that column. A second click should sort messages in ascending order. Note that an asterick appears to indicate the column criteria by which the entries are currently being sorted.

Click the appropriate column header (link) to sort the entries by that criteria

Note that an asterisk appears to indicate how the information is currently sorted



5. I-Gear Administration

I-Gear's administrative functions are performed through a standard Web browser such as Netscape Navigator or Microsoft Internet Explorer. The administrative interface is based on the I-Gear objects and methods described in "The I-Gear Design" on page 3.

If you have not purchased the Enterprise version of I-Gear, I-Gear's administrative functions are performed using the standard interface.

If you have purchased the Enterprise version of I-Gear, you can assign hierarchical administrative permissions to certain objects. You have two administrative interfaces available for use: the standard I-Gear interface and a family interface. The standard interface is the default interface for Users and Casts with administrative permissions. If you want the family interface to be used, you must assign this interface to a given object using the Modify method for that object.

Accessing the Administrative Functions

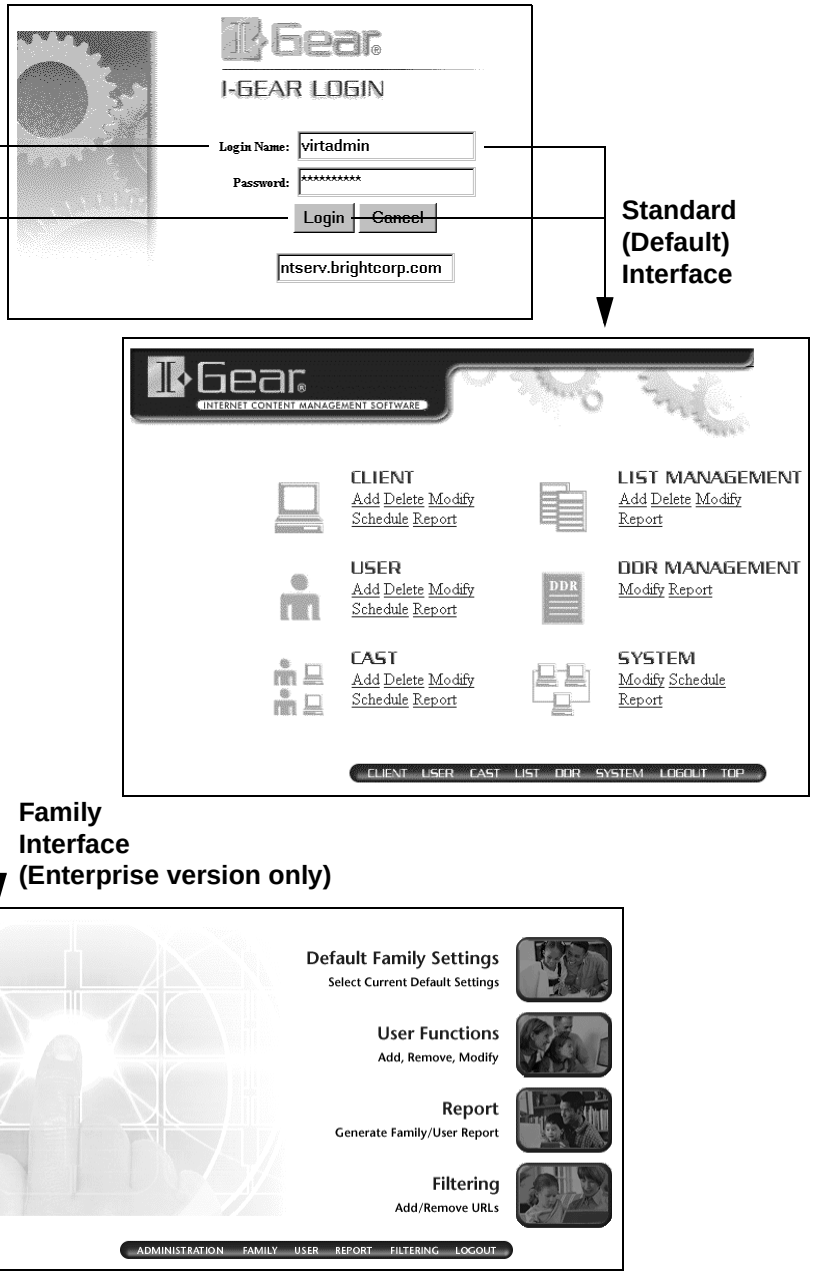
After installing I-Gear, launch a Web browser on any computer system on your network that can access the server running I-Gear. To access the I-Gear administrative interface, click the **I-Gear** button on the I-Gear tool bar or visit the URL

```
http://<servername>:port/admin
```

Enter the login name and password for an account that has administrative privileges, and click the **Login** button. The appropriate administrative interface (i.e., the interface that has been assigned to the logged-in User) will display.

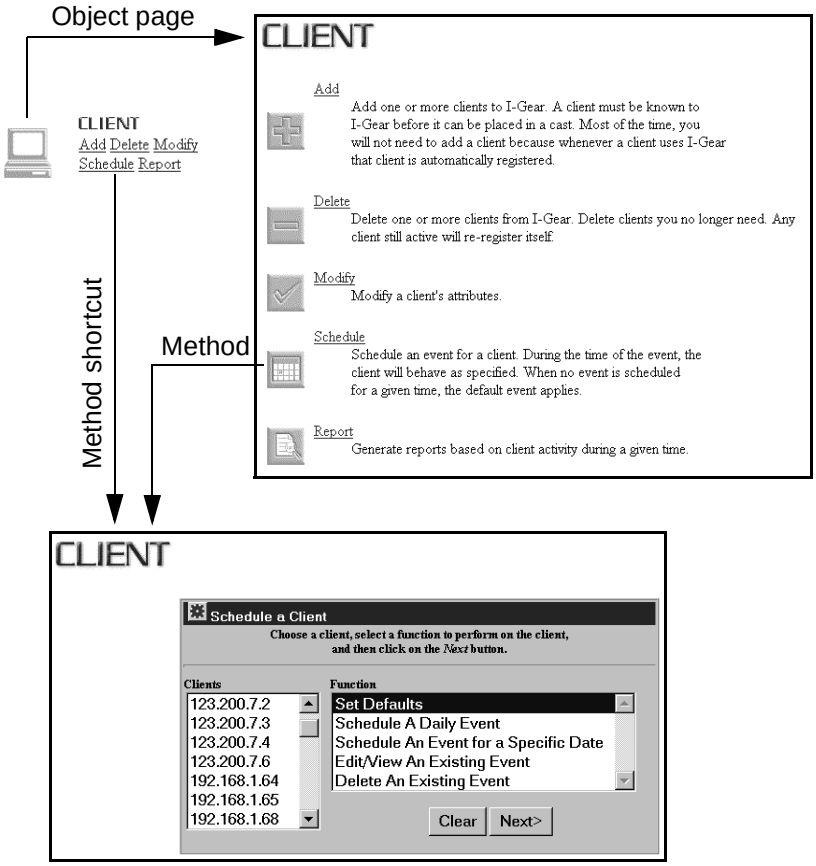
Note: At installation, I-Gear creates a virtual account with all global administrative privileges set. Initially, you must log on using this account to create your account and grant administrative privileges to this account. The User name for the virtual account is `virtadmin`. At

installation, if you followed the on-screen prompts, you should have entered your own password for this account.



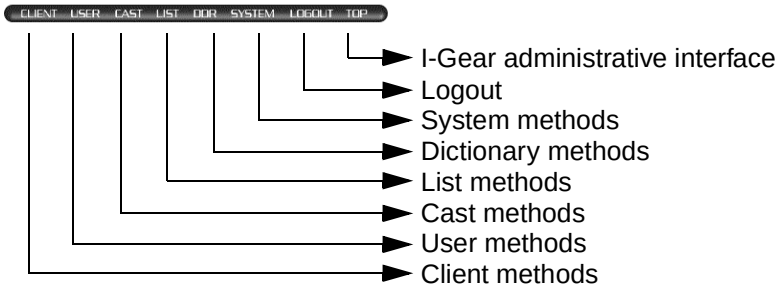
Standard (Default) Administrative Interface

The standard (default) I-Gear Administrative Interface contains icons for each object. You can click any of the object icons to display the object page. From the object page, you can access any method for that object. You can also use the method shortcuts, which appear next to each object icon. Only those methods applicable for a given object appear next to that object. If you do not have permission to perform a particular method for an object, the method is "grayed out" on both the main I-Gear administrative page and the object page.


Object page
CLIENT
Add Delete Modify
Schedule Report
Method shortcut
Method
CLIENT
Add
Add one or more clients to I-Gear. A client must be known to I-Gear before it can be placed in a cast. Most of the time, you will not need to add a client because whenever a client uses I-Gear that client is automatically registered.
Delete
Delete one or more clients from I-Gear. Delete clients you no longer need. Any client still active will re-register itself.
Modify
Modify a client's attributes.
Schedule
Schedule an event for a client. During the time of the event, the client will behave as specified. When no event is scheduled for a given time, the default event applies.
Report
Generate reports based on client activity during a given time.
CLIENT
Schedule a Client
Choose a client, select a function to perform on the client, and then click on the Next button.
Clients
123.200.7.2
123.200.7.3
123.200.7.4
123.200.7.6
192.168.1.64
192.168.1.65
192.168.1.68
Function
Set Defaults
Schedule A Daily Event
Schedule An Event for a Specific Date
Edit/View An Existing Event
Delete An Existing Event
Clear
Next>

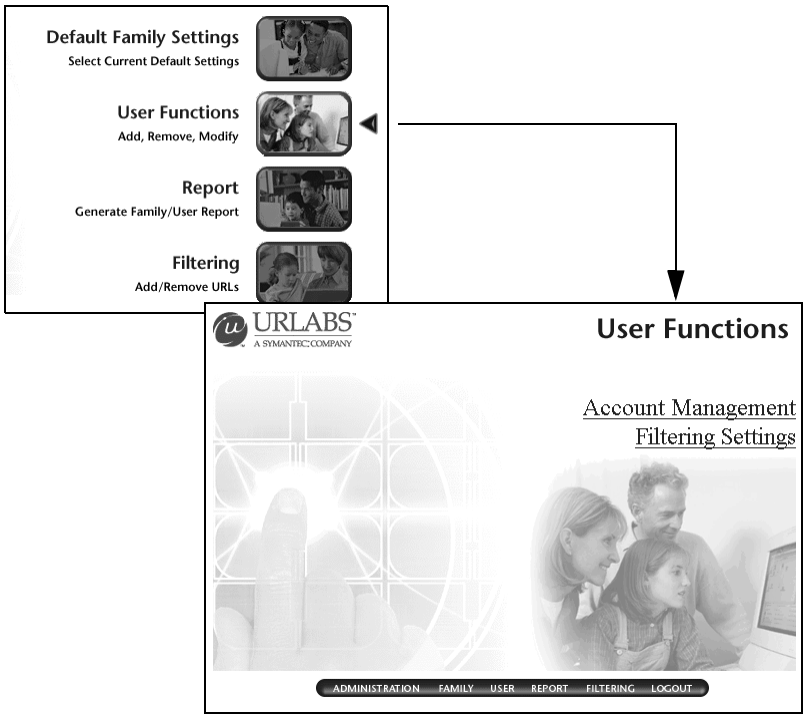
The trailing tool bar located at the bottom of most administrative pages also can be used to quickly access various sections of the I-Gear package. You can use this tool bar from most administrative pages to keep

from having to return to the I-Gear Administrative Interface each time you want to perform a new function.

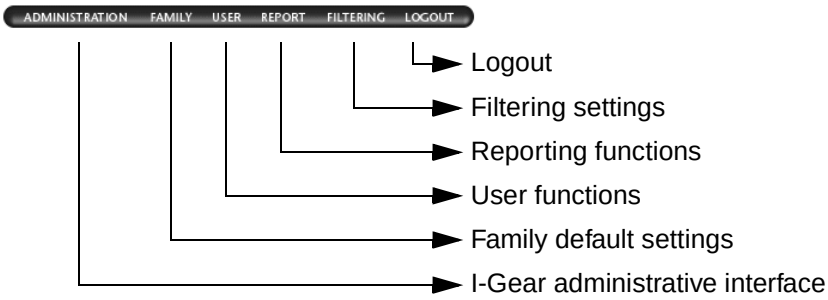


Family Interface (Enterprise version only)

The family I-Gear Administrative Interface is broken down into four functional areas: Default Family Settings, User Functions, Report Functions, and Filtering. You can click on any of these hyperlinks to perform a related function. If a User does not have permission to perform a particular function, that function does not appear for that User.

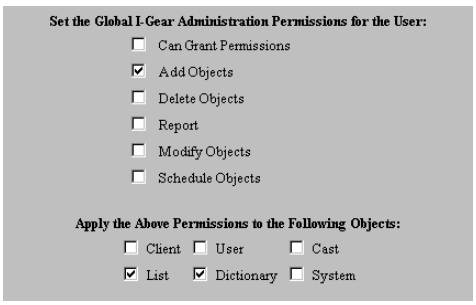


The trailing tool bar located at the bottom of most administrative pages also can be used to quickly access various sections of the family interface. You can use this tool bar from most administrative pages to keep from having to return to the main administration page each time you want to perform a new function.



Global Administrative Permissions

Global permissions for administering I-Gear are assigned using the Modify method for the User object. (See “Modifying Attributes” on page 89 for more information.) Global permissions can also be assigned at the same time a new User account is created if you use the advanced User creation setting. (See “Adding One User at a Time (Advanced)” on page 85 for more information.) Global permissions can be assigned based on both object and method. For example, a User could be given permission to Add objects, but only be given permission to apply the Add method to List and Dictionary objects. This User, then, would be unable to add new Users or Casts, but could create new Lists and Dictionaries as needed.



Global permissions apply to all objects. For example, if a User has global permission to schedule Users and Casts, that User is allowed to schedule *any* existing User and Cast in I-Gear.

Hierarchical Administration (Enterprise version only)

The Enterprise version of I-Gear provides two levels of administrative permissions: global permissions and Access Control permissions. *Global* permissions permit the overall administration of I-Gear. For example, Users with global permissions for modifying Casts can modify any existing Cast in I-Gear. *Access Control* permissions allow a User to perform administrative functions only for those objects (Users, Casts, Clients, or Lists) for which they have been given specific control. So a User who has been placed on the Access Control List for a given Cast (with appropriate permissions) can modify only that Cast, as well as that Cast's individual members.

The Access Control List feature allows you to delegate some administrative permissions to selected Users for certain objects without having to release global control of I-Gear. Managers can be given administrative responsibility for their employees, teachers can be given responsibility for certain students or for the workstations in a particular classroom, and ISPs can delegate responsibility for managing multiple family-member accounts to the head of household.

Although you are able to delegate administrative permissions to certain Users, I-Gear still allows you to implement general acceptable-use policy settings that apply to all Users. Even Users who have been granted certain Access Control permissions (e.g., scheduling permissions) can be prevented from overriding certain filtering settings that have been established (e.g., so that a manager would not be able to schedule a favored employee for unfiltered access).

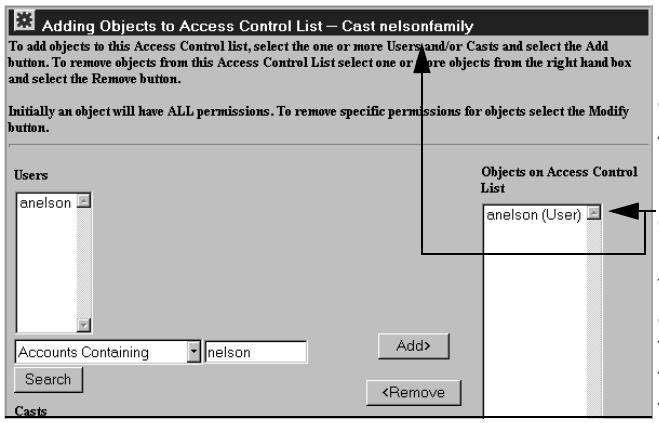
Access Control Lists

Any Client, User, Cast, or List object can have an associated Access Control List. Both Users and Casts can be placed on Access Control Lists. Any User or member of a Cast that is on an Access Control List for an object is allowed to perform administrative functions for that object. The particular administrative permissions that can be performed are based on the Access Control List permissions that are individually granted to members of each Access Control List. Access Control permissions apply only to the object to which the particular Access Control List belongs. For example, a User could actually be on several Access Control Lists for different objects, and the permissions might be different for each object. For example, a manager might be placed on two Access Control Lists for two different Casts and have all permissions for one Cast and only reporting capability for the other Cast.

Note: An object does not need to have an Access Control List. If no Access Control List is active for an object, that object can only be controlled by Users with the appropriate global permissions.

Users and Casts are placed on an object's Access Control List using the Modify method for that object. See "Adding/Deleting Objects to/from the Access Control List (Enterprise version only)" on page 53 for more information. Access Control List permissions are assigned to members of an object's Access Control List using the Modify method for that object. See "Modifying Permissions on Access Control List (Enterprise version only)" on page 55 for additional information.

In general, the Access Control List feature is intended to be utilized in a manner similar to the following example. A User or Cast (in this example, the User `anelson`) is placed on an Access Control List for a particular Cast (here, the `nelsonfamily` Cast) and assigned certain permissions that allow the User to manipulate that Cast and its members. Thus, the User potentially is able to Delete, Modify, Schedule, and Report on the members in that Cast.


Adding Objects to Access Control List – Cast nelsonfamily
To add objects to this Access Control list, select the one or more Users and/or Casts and select the Add button. To remove objects from this Access Control List select one or more objects from the right hand box and select the Remove button.
Initially an object will have ALL permissions. To remove specific permissions for objects select the Modify button.
Users
anelson
Objects on Access Control List
anelson (User)
Accounts Containing
nelson
Search
Add>
<Remove
Casts

Here, `anelson` has been added to the Access Control List for the `nelsonfamily` Cast; thus, this User can apply the permissions assigned below to perform certain functions for this Cast

Here, `anelson` has been given all Access Control permissions for the `nelsonfamily`Cast

Note: When a Cast is placed on an Access Control List for an object, any member of that Cast is able to control the object (based on the assigned permissions). For example, a Cast `Administrators` is placed on an Access Control List for another Cast `12thgraders`. In this scenario, any member of the `Administrators` Cast can control the `12thgrade` Cast as a whole or any member of the `12thgrade` Cast individually.

Object Creation/Modification Quotas

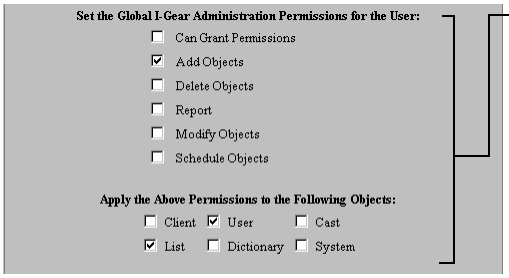
Quotas also can be established for individuals who have global permissions to add Users and Lists to I-Gear. Quotas can be set for the number of new Users that can be added, the number of new Lists that can be added, and for the total number of URLs that can be added to all Lists by that User. This feature is not limited to the Enterprise version; however, it can easily be used in conjunction with Access Control Lists to allow greater delegation of responsibility in managing accounts. In the above example, a head of household (`anelson`) has been placed on the Access Control List for the family Cast (`nelsonfamily`). Now, as head of household, the ISP could allow `anelson` to create 4 additional Users for other family members and up to 10 different Lists for customized filtering for family members. Furthermore, the ISP could set up `anelson`'s account so that `anelson` is automatically added to the Access Control List for all Users and List created by the head of household.

To add new Lists and Users, `anelson` must be granted global permissions for adding Lists and Users. For guidance on granting global permissions, see the section entitled "Modifying Attributes" on page 89. Next, the quotas for `anelson`'s account must be set. See "Modifying Object Creation/Modification Attributes" on page 92 for more information on establishing object creation quotas.

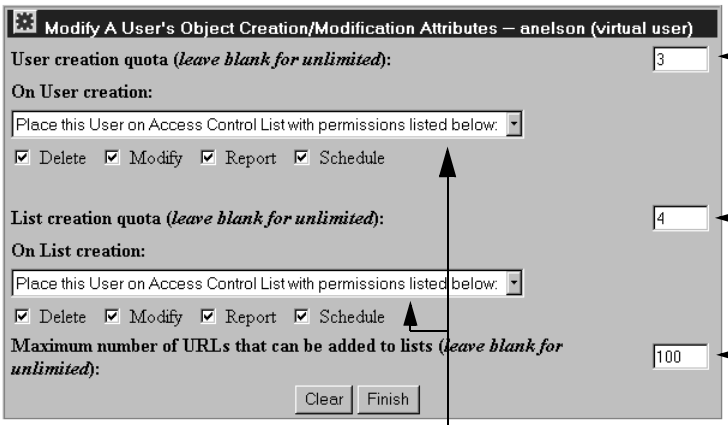
Note: The account for a User who has permission to add new Users and filter Lists can be set up so that the User is automatically added to the Access Control List (with appropriate permissions) for the newly created object. (This feature is only applicable to the Enterprise version of the software.)

Note: When a User (who is on the Access Control List for a Cast and is a member of that Cast) uses the Family interface to create new Users, the new Users are automatically added to the Cast. If the standard (default) interface is used, the new Users are NOT automatically added

to the same Cast. Thus, with the standard interface, this step must be accomplished manually.



If anelson is to create new Users or Lists for the nelsonfamily Cast, he must also be given global permissions for the Add method for both User and List objects



In addition, anelson's account has been set up so that anelson is automatically added to the Access Control List with the appropriate permissions for each new User and List created by this User

Here, User and List creation quotas have been established for anelson, and the maximum number of URLs that can be added to each new list has been established

Preventing Filtering Overrides

Because filtering settings can get rather complex with both Access Control and global permissions, I-Gear provides several safeguards to prevent Users with relevant permissions from overriding certain filtering settings that have been established by a particular site.

I-Gear allows you to restrict individual Users or all Users with appropriate scheduling permissions from being able to schedule other Users for unfiltered access or for Audit Mode. You can prevent an individual from scheduling unfiltered access using the Modify method for the User

object. For more information, see the section entitled “Modifying Attributes” on page 89.

I-Gear also allows you to restrict Users from overriding the filtering state of a List. You can prevent Users from changing the state of any existing List in I-Gear using the Modify method for the List object. (For more information, see “Changing the Filtering Override Setting for a List” on page 112. This step can also be accomplished when a new List is first created in I-Gear.

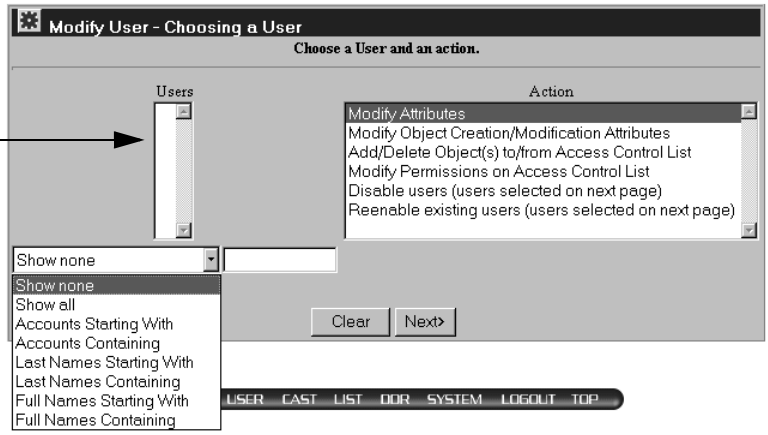
Search Capability for Object Lists

For I-Gear functions (e.g., Deleting or Modifying Clients, Users, Casts, or Lists) which require administrators to select objects from a list, I-Gear features a search capability. This search capability eliminates the need to scroll through a long list to locate a particular User or Client and can be useful for sites that are supporting large numbers of Users or Clients. This search capability can be turned on and off individually for each object. If the feature is turned on for a given object, the search fields display automatically wherever necessary in the appropriate I-Gear displays. When turned off, the search fields do not display. For instructions on activating this feature, see the section entitled “Modifying Object Box Controls” on page 128.

In addition to the search capability, you can also specify whether to automatically display all of the objects in a given list (Show All) or to show no objects until search results are posted (Show None). This feature can be useful for sites that have large numbers of system Users. By choosing not to show Users by default, you can eliminate a potential delay that may be incurred because I-Gear must request this information from the system. For guidance on choosing whether or not to display the complete List of Users by default, see the section entitled “Modifying Object Box Controls” on page 128.

When a screen with active search capability is first displayed, the pull-down menu on the left displays the Show All or Show None default set-

ting. To use the search capability, select a search parameter from this pull-down menu.



In this case, **Show None** is the default setting; thus, the list of Users contains no entries until search results are displayed

If the default setting was **Show All**, the complete list of Users would display

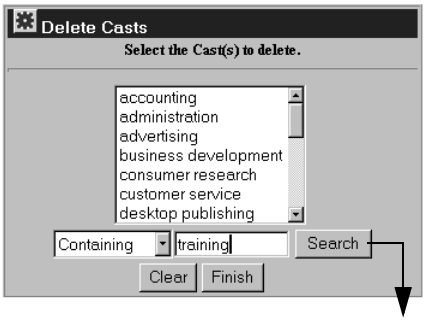
The search parameters for the User object differ from those for other objects. The search parameters for the User object are described in the table below.

Parameter	Description
Accounts Starting With	I-Gear will search for all account names that start with given text.
Accounts Containing	I-Gear will search for all account names that contain given text.
Last Names Starting With	I-Gear will search for all User last names that start with given text.
Last Names Containing	I-Gear will search for all User last names that contain given text.
Full Names Starting With	I-Gear will search for all User names (including first names) that start with given text.
Full Names Containing	I-Gear will search for all User names (including first names) that contain given text.

The search parameters for Client, Cast, and List objects are described in the table below.

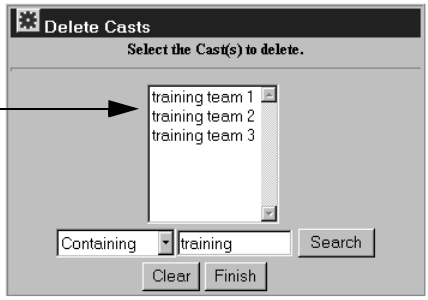
Parameter	Description
Starting With	I-Gear will search for all entries that start with given text.
Containing	I-Gear will search for all entries that contain given text.

After you have selected a search parameter, enter in the field on the right side of the search display the accompanying text for which I-Gear will search. Then click the **Search** button.



Enter the desired search parameter and text, and then click the **Search** button

In this case, the search has returned three Cast entries that contain the desired text “training” (the returned results appear in the list field)



Highlight the appropriate entries returned in the search, and continue with the desired function (in this case, deleting a Cast)

I-Gear will display the search results in the object list field. Highlight the appropriate entries in the results and continue with the function you are performing. Note that even if only one entry is returned you will still need to highlight this entry in order to proceed.

Editing the Access Denied Page

The I-Gear Access Denied page can be customized to suit your local needs. To customize the Access Denied page, you must edit two local configuration files: `blocked.mhtml` and `blocked.txt`. The `blocked.mhtml` file is used for the Access Denied page when the browser is able to display an HTML document, and the `blocked.txt` file is used when only a text file can be displayed. (The file that is displayed is dependent on the type of file the browser is working on when the Access Denied page is needed. Thus, both files should be edited to be the same so that your Access Denied message is consistent.) At installation, you were prompted to indicate a directory for the local configuration files. These two files should be located in this directory.

Warning: The two files noted above are the only two files that you are licensed to modify. Any HTML modifications beyond those described here require a separate license from URLabs. If you feel you need to modify other HTML files, contact a URLabs representative for more information. Unauthorized modification to the software is addressed in the Software License Agreement at the front of this manual.

The Access Denied page contains text that remains the same each time the page is displayed, as well as dynamic information specific to the blocked event (e.g., the reason the user has been blocked, the requested URL). Both the standard and the dynamic text can be changed as necessary using HTML editing convention.

Edit the standard text as appropriate. To insert the dynamic information where appropriate, you will need to use the following HTML tags.

%%R - displays reason that requested site was blocked (e.g., DDR, Allow Only, Deny List)

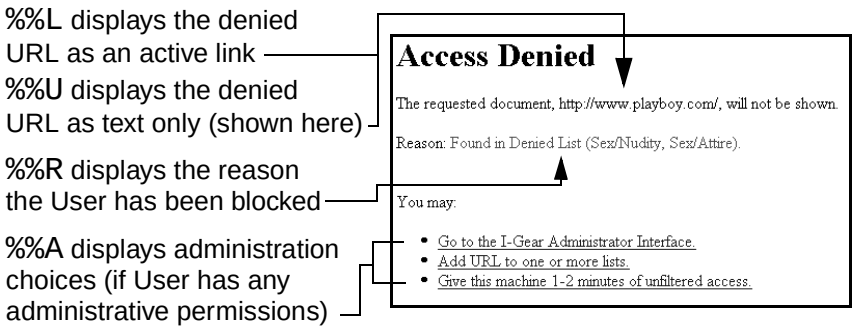
%%F - displays words found by DDR that resulted in page being blocked

%%A - displays administrative options (only for users with administrative permissions)

%%H - inserts name of host running I-Gear (to enable you to construct any desired local links)

%%L - displays denied URL as an active link

%%U - displays denied URL as text only (not as an active link)


%%L displays the denied URL as an active link
%%U displays the denied URL as text only (shown here)
%%R displays the reason the User has been blocked
%%A displays administration choices (if User has any administrative permissions)
Access Denied
The requested document, http://www.playboy.com/, will not be shown.
Reason: Found in Denied List (Sex/Nudity, Sex/Attire).
You may:
Go to the I-Gear Administrator Interface.
Add URL to one or more lists.
Give this machine 1-2 minutes of unfiltered access.

6. Working with the Client Object

Adding a Client

To add a Client object to I-Gear, click the Add link from the Client object administration page or the Client Add shortcut from the main I-Gear administration page.

When a Client computer has its proxy settings for Internet use set to the server running I-Gear, the Client is automatically added to the I-Gear Client database when the Client first receives an I-Gear login page. The Client's IP address will first appear in the Unauthorized Client List on the left. Based on your licensing agreement, you may need to identify Clients authorized to use I-Gear (see the notes below).

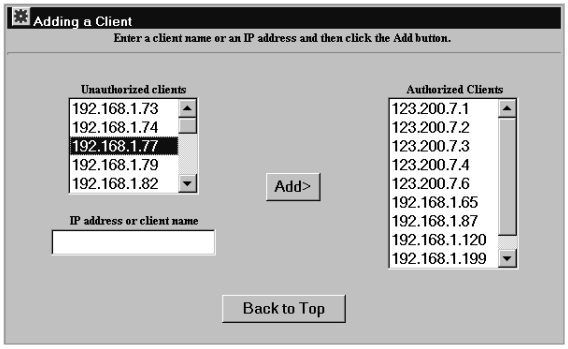
Note: If your licensing agreement does not specify a limit on the number of authorized Clients, you do not have to worry whether Clients are authorized or unauthorized. However, if you are limited to a certain number of authorized Clients, you will need to authorize the appropriate Clients to use I-Gear.

Note: If your licensing agreement does NOT limit the number of authorized Clients, you can still activate the authorized/unauthorized Client feature if desired. This feature can be used to allow only the Clients that have been authorized to access I-Gear; thus, you could prevent certain machines from being able to access I-Gear by leaving the appropriate IP addresses in the unauthorized state. For information on activating this feature, see "Modifying Other Settings" on page 130. Once you have activated this feature, you will need to authorize the appropriate Clients using the Add method for the Client object.

To authorize a Client to use I-Gear, select the appropriate Client IP address from the List on the left and click the **Add** button. The IP address should now appear in the Authorized Client list on the right side of the display. You can continue to authorize Clients until you reach the limit specified in your licensing agreement. If you have more Clients on your network than your licensing agreement allows, you will need to move Clients back and forth from Authorized to Unauthorized status (using the Add and Delete methods for the Client object) as necessary.

If a particular Client has not accessed the server since I-Gear has been installed, the Client also can be added manually. In the space provided, enter the Client's IP address or the name of the Client. Then click the

Add button. The IP address should now appear in the Authorized Clients list. If you enter the machine name, I-Gear will automatically convert the machine name and display the IP address in the List.



Note: You also can authorize a range of Client IP addresses at once. For example, to add the IP addresses 192.168.1.1 through 192.168.1.100, type the following range into the IP Address/Client Name field: `192.168.1.1 - 192.168.1.100`. Then click the **Finish** button. If you are familiar with the Classless Inter-Domain Routing (CIDR) representation, you can also use this notation to specify a range of Client IP addresses to I-Gear.

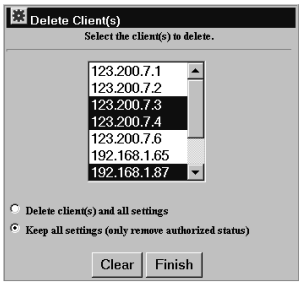
When you have finished adding Clients, click the **Back to Top** button to return to the I-Gear administration page.

Deleting a Client

To delete a Client object within I-Gear, click the Delete link from the Client administration page or the Client Delete shortcut from the main I-Gear administration page.

Select the IP address(es) you wish to delete. Also select whether you wish to delete the Client and all associated settings completely from I-Gear or simply remove the Client's authorized status and retain the associated settings. If you remove the Client's authorized status but retain the associated settings, the Client's Cast, the default settings, and any scheduled events are retained by I-Gear. After you have made the appropriate selection, click the **Finish** button.

You can select more than one Client at a time, usually by holding down the **Control** key while selecting multiple IP addresses. Use the **Clear** button to deselect all IP addresses and clear the display.



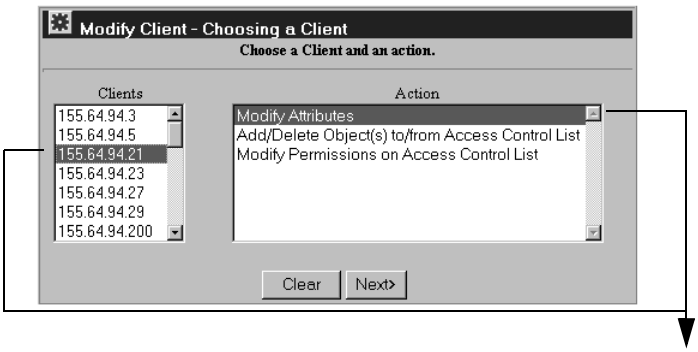
Modifying a Client

The Modify method for the Client object allows you to specify a Cast, the type of browsing activity that will be logged, the default URL, and the default administrative interface for the selected Client. If you have purchased the Enterprise version of I-Gear, you can also modify the Access Control List features for the Client.

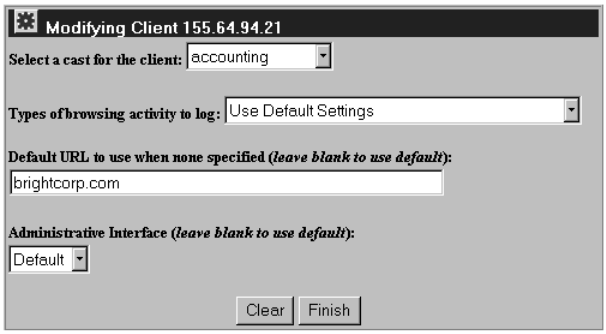
To modify a Client, click the Modify link from the Client object administration page or the Client Modify shortcut from the main I-Gear administration page.

Modifying Attributes

To modify the attributes for a selected Client, select the IP address of the Client you wish to modify, select Modify Attributes from the menu provided, and click the **Next** button.



From the next display, first select the Cast for the Client. Selecting the blank space will place the Client in a state of not belonging to any Cast.



Then select the type of browsing activity that will be logged for the Client. You do not need to specify activity logging for individual Clients unless the logging requirements for the Client differ from inherited default settings. Clients inherit other default settings for activity logging, subject to the hierarchy of permissions discussed in "The I-Gear Design" on page 3. If you do not need to change the Client's settings, select Use Default Settings. If you do need to change the Client's settings, select the appropriate level of activity logging.

Warning: Many of the Report functions will not operate if activity logging is disabled. For example, if you select no activity logging for a particular Client and you have assigned Client settings with the highest priority in I-Gear, then a report generated for a given User (for whom you normally log browsing activity) would contain no information on the User's browsing activity if the User used that Client (because Client permissions would have the highest priority).

Specify the default URL to display for the Client when no other URL has been requested (i.e., the URL that the browser will display automatically after a User clicks the **Login** button). You do not need to specify a default URL for an individual Client unless the URL for the Client differs from the inherited default settings.

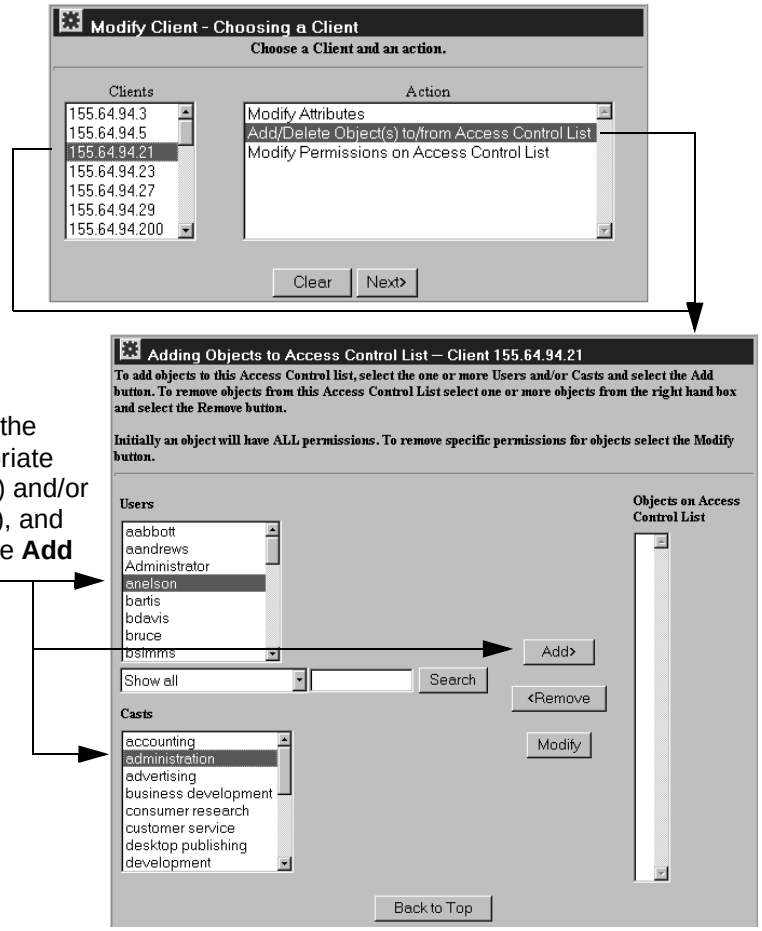
If you have the Enterprise version of the software, you also must specify the administrative interface (either the standard or the family interface) to be displayed when a User with administrative permissions accesses the I-Gear administrative interface from the selected Client. (Note that the interface that actually is displayed will depend on the hierarchy of permissions that has been established for I-Gear and the settings for the particular User.) If you select Use Defaults, the Client will inherit other

applicable default settings for the administrative interface, subject to the hierarchy of permissions.

When you have completed your changes, click the **Finish** button. I-Gear will provide confirmation that your changes have been made.

Adding/Deleting Objects to/from the Access Control List (Enterprise version only)

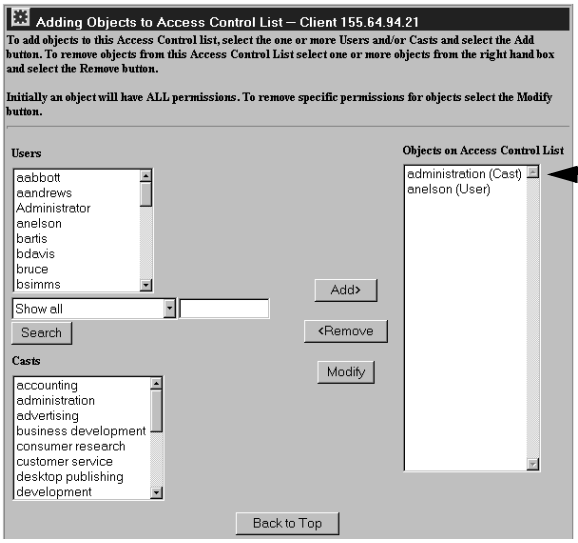
To add or delete objects from the Access Control List for a selected Client, select the IP address of the Client you wish to modify, select Add/Delete Objects to/from Access Control List, and click the **Next** button.



Select the appropriate User(s) and/or Cast(s), and click the **Add** button

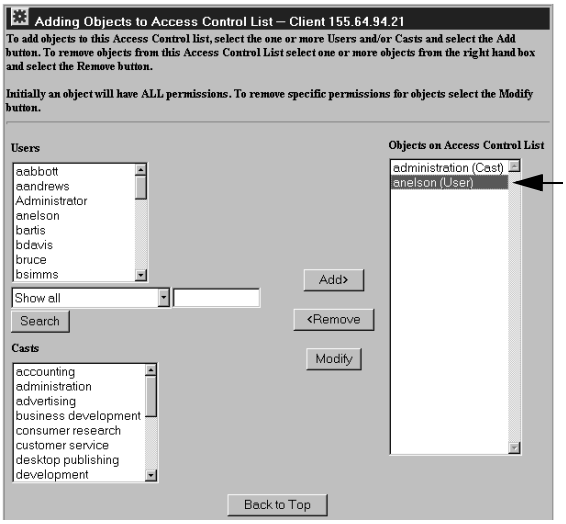
You may add as many Users or Casts as necessary to the Access Control List. The left side of the display shows lists of both I-Gear Users and

Casts. To add Users or Casts to the Access Control List for the selected Client, select the appropriate objects from either or both lists on the left side of the display, and click the **Add** button. The Access Control List on the right side of the display should update to reflect your changes.



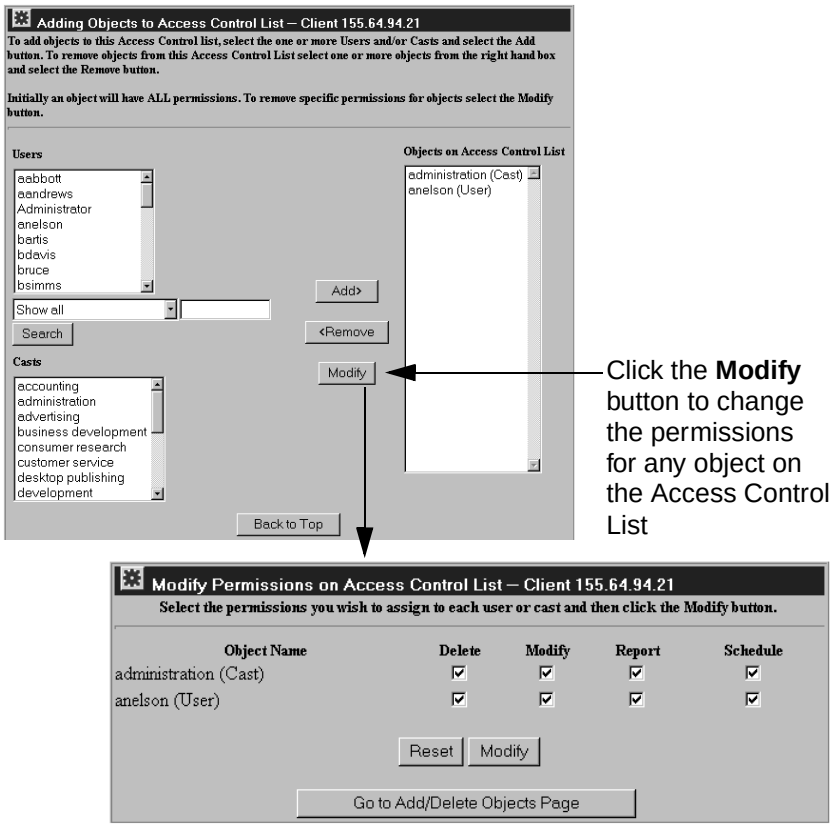
The display should update to reflect your changes

You can also delete User and Cast objects from an Access Control List from this display. The objects currently on the Access Control List for the selected Client are shown on the right side of the display. To delete an object from the Access Control List, select the object(s) to be removed from the list on the right side of the display, and click the **Remove** button. The display should update to reflect your changes.



Highlight the object to be removed from the Access Control List and click the **Remove** button

When a User or Cast object is first added to a Client's Access Control List, that object is automatically granted all permissions for controlling the selected Client. If you want to change the permissions for an object on an Access Control List, click the **Modify** button.

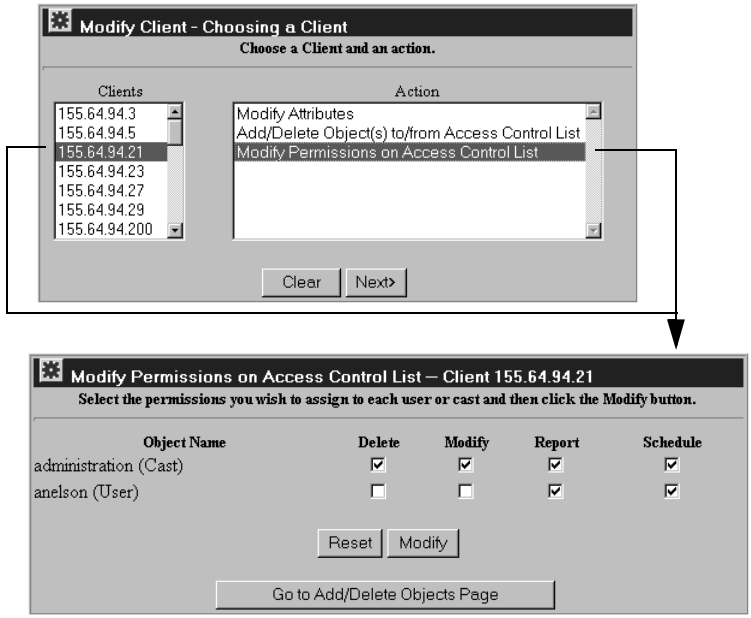

Adding Objects to Access Control List – Client 155.64.94.21
To add objects to this Access Control list, select the one or more Users and/or Casts and select the Add button. To remove objects from this Access Control List select one or more objects from the right hand box and select the Remove button.
Initially an object will have ALL permissions. To remove specific permissions for objects select the Modify button.
Users
aabbott
aandrews
Administrator
anelson
bartis
bdavis
bruce
bsimms
Show all
Search
Casts
accounting
administration
advertising
business development
consumer research
customer service
desktop publishing
development
Add>
<Remove
Modify
Back to Top
Objects on Access Control List
administration (Cast)
anelson (User)
Click the Modify button to change the permissions for any object on the Access Control List
Modify Permissions on Access Control List – Client 155.64.94.21
Select the permissions you wish to assign to each user or cast and then click the Modify button.
Object Name
Delete
Modify
Report
Schedule
administration (Cast)
anelson (User)
Reset
Modify
Go to Add/Delete Objects Page

The next display shows the permissions for all members of the Access Control List. Assign the desired permissions for each member of the Access Control List by selecting the appropriate check boxes. Clicking the **Reset** button clears the display and resets the permissions to the currently saved settings. Click the **Modify** button when you are ready to save your changes. I-Gear will provide confirmation that your changes have been made.

Modifying Permissions on Access Control List (Enterprise version only)

To modify the permissions on the Access Control List for a selected Client, select the IP address of the Client you wish to modify, select Modify

Permissions on Access Control List from the menu provided, and click the **Next** button.

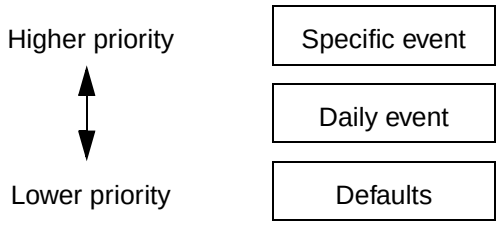


The next display shows the permissions for all objects that are currently on the Access Control List for the selected Client. Assign the desired permissions for each member of the Access Control List by selecting the appropriate check boxes. Clicking the **Reset** button clears any changes you have made on the display and resets the permissions to the currently saved settings. If you want to add or delete an object from the Access Control List, click the **Go to Add/Delete Objects Page** button. (You can return to this page by clicking the **Modify** button from that display.) Click the **Modify** button when you are ready to save your changes. I-Gear will provide confirmation that your changes have been made.

Scheduling an Event for a Client

Scheduling events with the Schedule method is basically the same for Client, User, Cast, and System objects. Before you schedule events, you should be familiar with the priorities that I-Gear assigns to object per-

missions and to the different types of events, as discussed in the appropriately titled subsections in “The I-Gear Design” on page 3.



Specific events are scheduled for a specific date and time, such as 10/28/1997 from 2:00 PM to 3:00 PM. Daily events reoccur each specified day, such as every Monday and Wednesday from 11:00 AM to 1:00 PM. Default settings apply when no other event is in effect.

Note: Keep in mind when scheduling a Client that by default Client permissions have the highest priority. If you have not changed I-Gear’s default settings for hierarchy of permissions, events scheduled for a Client will affect any User who uses the Client during the event.

To schedule a Client, click the Schedule link from the Client object administration page or the Client’s Schedule shortcut from the main I-Gear administration page.

Setting Defaults

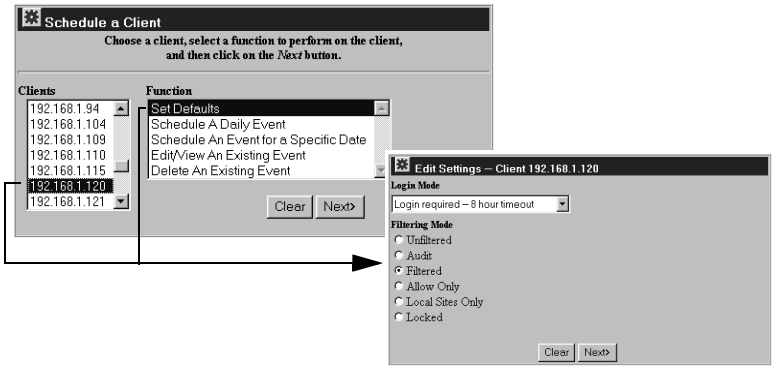
Note: Only the System object must have default settings. Other objects can be scheduled for specific or daily events and fall back to the system default settings when no other event is in effect.

Note: Different default access permissions can be scheduled for the System object and other Users, Clients, and Casts. This feature gives you the flexibility, for example, to make filtering options less strict for adults than for young children. Furthermore, you can design your network in such a way that individuals must be at certain Clients to download certain file types.

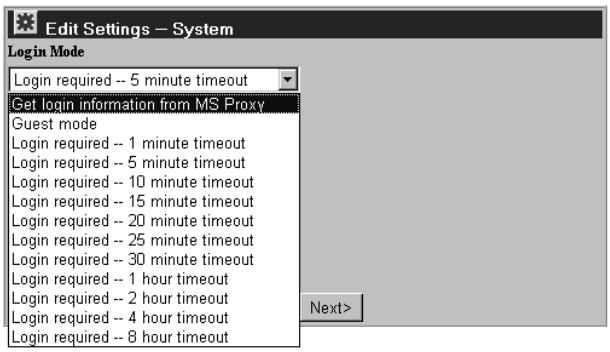
To change the default access permissions for a Client, select the appropriate Client, select the Set Defaults function, and click the **Next** button.

From the next display, first select the desired login behavior from the menu. Select a particular time-out period (i.e., the period of inactivity after which I-Gear will automatically log the current User out) from the selections provided. You also can turn off the login requirement by put-

ting the Client into Guest Mode. (Depending on your I-Gear licensing scheme, the Guest Mode feature may not be available.)



If you are running I-Gear for MS Proxy, you can also select Get Login Information from MS Proxy for the desired login behavior. The Get Login Information from MS Proxy setting is provided for sites wanting to use the authentication capability of IIS and Microsoft Proxy (such as NT Challenge/Response authentication) instead of the login functionality provided with I-Gear. This option allows the browser to obtain login information directly from IIS rather than requiring the user to log directly into I-Gear. See the section entitled “Logging In” on page 28 for more information.


Edit Settings – System
Login Mode
Login required -- 5 minute timeout
Get login information from MS Proxy
Guest mode
Login required -- 1 minute timeout
Login required -- 5 minute timeout
Login required -- 10 minute timeout
Login required -- 15 minute timeout
Login required -- 20 minute timeout
Login required -- 25 minute timeout
Login required -- 30 minute timeout
Login required -- 1 hour timeout
Login required -- 2 hour timeout
Login required -- 4 hour timeout
Login required -- 8 hour timeout
Next>

Note: Access to I-Gear’s administrative interface will require the User to log directly into I-Gear regardless of whether the Get Login Information from MS Proxy option has been selected.

Note: If the Get Login Information from MS Proxy option is selected, you also **must** enable access control in Microsoft Proxy. Failure to do so could result in unfiltered access. (See Microsoft Proxy Server documentation for information on how to enable access control.)

Note: The Get Login Information from MS Proxy option is not recommended when initially configuring I-Gear for MS Proxy. Correct operation of I-Gear for MS Proxy should be verified first using either Login Required or Guest mode. After correct operation has been verified, you can change to Get Login Information from MS Proxy, if desired.

After you have selected the appropriate login behavior, next select the desired level of filtering from the following choices.

- **Unfiltered.** No filtering is done on Internet materials accessed.
- **Audit.** The User is not blocked from accessing inappropriate content. The attempt is logged as though the User has been prevented from accessing the content; however, access to the inappropriate material is permitted. Thus, Audit mode is transparent to the User; however, by reporting on the activity for that User, the User's access activity can be monitored.
- **Filtered.** Attempts to access Internet materials are subject to the filtering guidelines that have been established. (Specification of inappropriate content is done from the next screen.) In Filtered mode, any attempt to access inappropriate content is logged, and the User receives a message to indicate that access to the inappropriate content has been blocked.
- **Allow Only.** Access is permitted only to those sites specifically designated as Allow (Filtering Enabled) or Allow (Filtering Disabled). (You can specify those lists to be allowed from the next screen.) Access to all other Internet sites is prevented.
- **Local Sites Only.** Access is permitted only to sites with the same Internet domain name as the server running I-Gear. Access to all other Internet sites is prevented.
- **Locked.** No Internet access is permitted. This option is typically used to deny Internet access for specific Users or Clients and is not normally used as a default system mode.

Select the desired filtering mode and click the **Next** button.

If you select Unfiltered, Locked, or Local Sites Only, you will receive confirmation that your changes have been made successfully. Click the **Done** button to return to the I-Gear administrative interface.

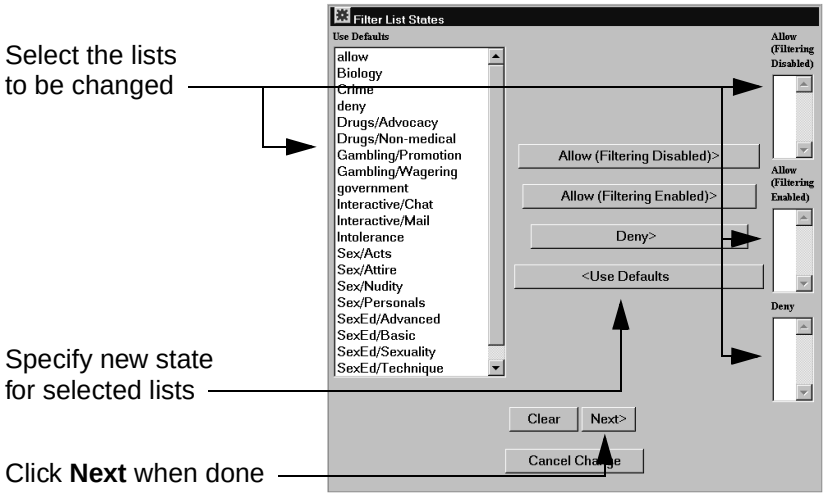
If you select Filtered, Audit, or Allow Only as the default filtering mode, you will be prompted to identify how the Category Lists are to be applied for filtering. (Each Category List includes both a List of related URLs and the associated Dictionary terms used by DDR.) The System is the only object that must have default settings; other objects automat-

ically inherit the System default settings unless you change the settings for that specific object. Thus, the Category Lists for Client, User, and Cast objects initially are shown under Use Defaults. If the default settings for certain Content Category Lists for a given object do not need to be different from the System default settings, these Lists can be left under the Use Defaults setting. If you need to change the Content Category List default settings for an object, select one of the following three states, as appropriate.

- **Allow (Filtering Enabled).** Category Lists in the Allow (Filtering Enabled) state specify content to which access is to be permitted. However, content specified by a Category List in the Allow (Filtering Enabled) state is still scanned by DDR. Furthermore, the Dictionary terms associated with categories in this state are NOT used by DDR in scoring content. Remember that if the system is in the Allow Only filtering mode, access will be permitted **only** to the content specified by Lists in either of the Allow states.
- **Allow (Filtering Disabled).** Category Lists in the Allow (Filtering Disabled) state specify content to which access is to be unconditionally permitted. Content specified by a Category List in the Allow (Filtering Disabled) state is **not** scanned by DDR, and the associated Dictionary is not activated. Additionally, if the System is in the Allow Only filtering mode, access will be permitted **only** to the content specified by lists in either of the Allow states.
- **Deny.** Category Lists in the Deny state specify content to which access is not permitted. The related terms found in the associated Dictionaries are used by DDR in scanning content for appropriateness.

Note: Lists can also be in the Off state for the System object. Category Lists in the Off state are not activated. The URLs in a Category List in the Off state are allowed (subject to other filtering, including DDR). Terms in the associated Dictionaries corresponding to Category Lists in the Off state are ignored by DDR in scanning content. Thus, Category Lists left in the Use Defaults state for a particular object and for which the System default setting is Off are also in the Off state for that object.

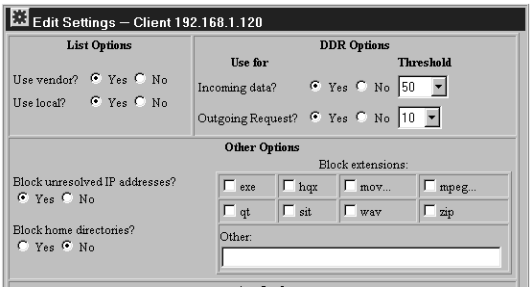
Most Category Lists are initially in the Off state when I-Gear is installed.



To specify the state of a Category List, select the List to be affected and click the **Deny**, **Allow (Filtering Enabled)**, **Allow (Filtering Disabled)**, or **Use Defaults** button, as appropriate. More than one List may be selected at a time, usually by holding down the control key while selecting the desired Lists—the exact method to select more than one List item is browser and operating-system dependent. When you have finished specifying the default state of the Category Lists, click the **Next** button.

From the next screen, you can establish other filtering options.

Note: If you have placed lists in the Allow (Filtering Disabled) state, the filtering options on this display do NOT apply in regard to those lists.



Set these additional filtering options, based on the following definitions:

Option	Description
Use vendor lists?	If “Yes” is selected, the object will be subject to the Allow and Deny Lists provided by URLabs (based on the selections made from the previous screen).
Use local lists?	If “Yes” is selected, the object will be subject to the local versions of the Allow and Deny Lists (based on the selections made from the previous screen).
Use DDR for incoming data?	If “Yes” is selected, DDR will scan documents accessed as they are being downloaded, unless the document URL appears in an active Allow (Filtering Disabled) List.
Use DDR for outgoing requests?	If “Yes” is selected, DDR will scan all outgoing requests (e.g., search strings). Because a search string would typically have fewer words, the DDR threshold for outgoing requests generally should be much lower than for incoming data. (See the next block in the table for information on selecting DDR thresholds.)
DDR Thresholds	If “Yes” has been selected for either or both DDR options, the DDR threshold(s) must be set. Certain words and phrases have been assigned point values, which DDR uses to score a Web page. With a lower threshold setting (i.e., lower numbers), the DDR sensitivity is increased, and pages that contain potentially inappropriate material are more likely to be blocked. Likewise, selecting a higher threshold (i.e., higher numbers) lessens the sensitivity of DDR and results in fewer potentially inappropriate pages being blocked. The default threshold values are 50 for incoming data and 10 for outgoing requests.
Block Unresolved IP Addresses?	If “Yes” is selected, requests for documents from remote servers for which the Internet domain name of the remote server cannot be determined will be blocked. **Note:** This option does not appear with I-Gear for FireWall-1.
Block Home Directories?	If “Yes” is selected, requests for URLs that contain the ~ (tilde) character, often used to represent personal Web spaces, will be blocked.

Option	Description
Block Extensions?	Access to documents can be blocked based on the extension of the document's URL. This option can be used to prevent specific document types from being downloaded. You can block additional extensions not listed by entering the extension (without a leading dot) in the Other box. More than one extension can be entered, each separated by a space. Note that some of the extensions listed end with "..." to indicate that more than one related extension is blocked. For example, "mov..." blocks both "mov" and "moov."

I-Gear's AutoLock and AutoAlert features can also be activated from this display.

If Filtered or Allow Only was selected as the filtering mode, the AutoLock feature can be activated if desired. (The AutoLock feature is not active in Audit mode.) I-Gear will automatically "lock" a User's account (i.e., suspend Internet access until the system administrator "unlocks" the account) if a specified number of blocked accesses are attempted within a given period of time. Two different methods are available for locking a User's account.

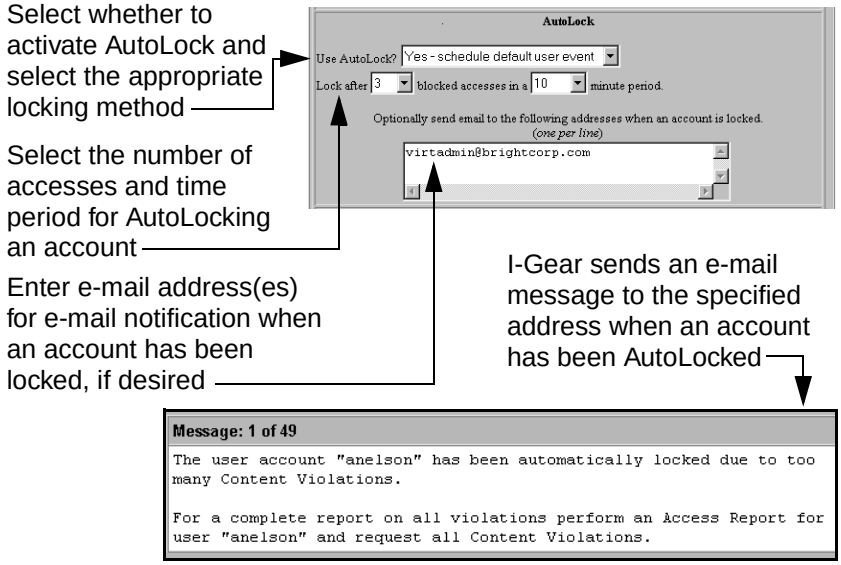
Locking method	Description
Schedule default user event	If you select "Yes - schedule default user event," a default event is scheduled for the User in which the User's filtering mode is set to locked. To UNLOCK the account, you must either delete or edit the event. **Note:** If you select this method for locking an account, the locked User may still have Internet access, depending on other, higher priority events that may be scheduled for the User or for the Client(s) used. For example, even though a student's account may be AutoLocked in this manner, the student would still have access from a Client that was scheduled to have Allow Only access for a certain research period. Thus, even though the account has been AutoLocked, the student is not prevented from completing normal studies during the period of time in which the account is locked. However, any Internet access that is not covered by a higher priority event would be prevented.

Locking method	Description
Disable user	If you select “Yes - disable user,” the User is disabled entirely from I-Gear. Thus, the User is prevented from logging into I-Gear, and ALL Internet access is denied. To UNLOCK the account, the User must be reenabled using the Modify method for the User object. **Note:** Disabling a User retains the User’s bookmarks, scheduled events, and other settings in I-Gear. If you are running other URLabs products (e.g., Mail-Gear) on the same machine as I-Gear and are taking advantage of the information-sharing capability between the products, disabling a User from I-Gear will not affect the settings in any other URLabs product. **Note:** Users who have the I-Gear administrative permission to Add Users cannot be AutoLocked in this manner. If you have selected this method for AutoLocking Users, this safeguard protects you from accidently having all Users with the permission needed to reenable Users locked out of I-Gear at the same time.

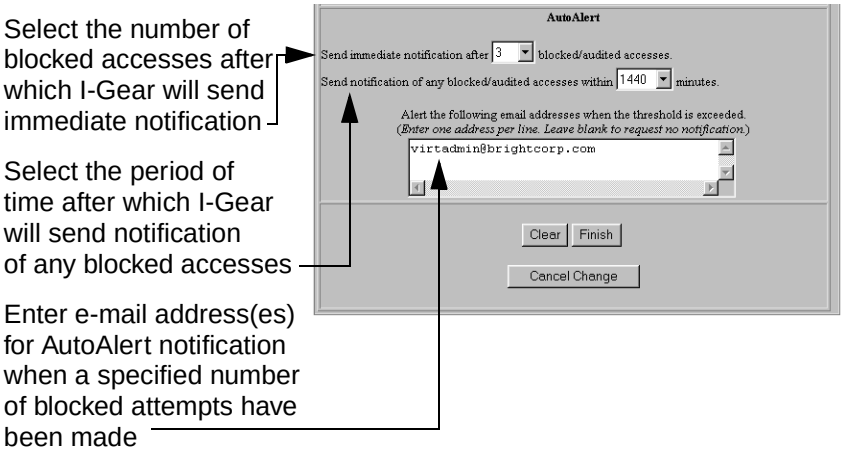
To activate the AutoLock feature, select “Yes” and the desired method for locking the account. Then select the number of blocked accesses that must occur and the time period in which these attempts must occur for an account to be AutoLocked.

To initiate automatic e-mail notification when an account has been AutoLocked, enter the appropriate e-mail address in the field provided. I-Gear automatically sends e-mail to the address(es) listed to indicate

that an account has been AutoLocked. If you do not want to activate the AutoLock notification feature, leave the e-mail notification field blank.


Select whether to activate AutoLock and select the appropriate locking method
Select the number of accesses and time period for AutoLocking an account
Enter e-mail address(es) for e-mail notification when an account has been locked, if desired
AutoLock
Use AutoLock? Yes - schedule default user event
Lock after 3 blocked accesses in a 10 minute period.
Optionally send email to the following addresses when an account is locked.
(one per line)
virtadmin@brightcorp.com
I-Gear sends an e-mail message to the specified address when an account has been AutoLocked
Message: 1 of 49
The user account "anelson" has been automatically locked due to too many Content Violations.
For a complete report on all violations perform an Access Report for user "anelson" and request all Content Violations.

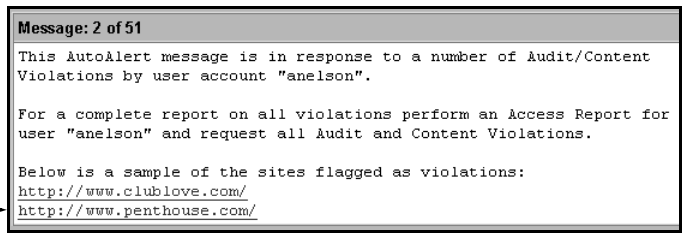
If you selected Filtered, Allow Only, or Audit mode as the filtering mode, you also can activate the AutoAlert feature from this display. I-Gear sends e-mail to the specified address(es) when a User attempts a specified number of blocked or audited accesses. I-Gear will automatically send e-mail to the address(es) listed in the field provided to indicate that a User has attempted to access restricted material.


Select the number of blocked accesses after which I-Gear will send immediate notification
Select the period of time after which I-Gear will send notification of any blocked accesses
Enter e-mail address(es) for AutoAlert notification when a specified number of blocked attempts have been made
AutoAlert
Send immediate notification after 3 blocked/audited accesses.
Send notification of any blocked/audited accesses within 1440 minutes.
Alert the following email addresses when the threshold is exceeded.
(Enter one address per line. Leave blank to request no notification.)
virtadmin@brightcorp.com
Clear
Finish
Cancel Change

To activate the AutoAlert feature, enter the appropriate e-mail address in the field provided. If you do not want to activate the AutoAlert feature,

leave this field blank. If you have activated AutoAlert, you must also select the number of blocked accesses that will result in immediate e-mail notification to the address(es) indicated. Then enter the amount of time after which I-Gear will provide notification of ANY blocked accesses.

The AutoAlert message lists a sample of the content and audit violations that resulted in the notification


Message: 2 of 51
This AutoAlert message is in response to a number of Audit/Content Violations by user account "anelson".
For a complete report on all violations perform an Access Report for user "anelson" and request all Audit and Content Violations.
Below is a sample of the sites flagged as violations:
http://www.clublove.com/
http://www.penthouse.com/

Note: The two AutoAlert parameters function somewhat independently of one another. That is, if the number of blocked accesses is set to 2 and the number of minutes is set to 30 and a User makes two blocked access attempts in a 30-minute period, then I-Gear will send a notification message immediately after the second attempt. However, if that same User makes only one blocked attempt in the same 30-minute period, then I-Gear still will send e-mail at the end of the 30-minute period to report the single blocked attempt. Thus, for sites with large numbers of Users, you may want to set the time period for notification to a larger block of time to limit the potential amount of e-mail received.

Note: The logging of browsing activity for AutoAlert is separate from I-Gear's regular activity logging. Thus, AutoAlert functions regardless of the settings you have established for normal activity logging. However, if normal activity logging is turned off, you will not be able to use I-Gear's reporting features to review the access attempts that resulted in the AutoAlert notification.

Note: The AutoAlert feature differs from the AutoLock feature in that AutoAlert functions when I-Gear is operating in Audit mode. Thus, you can set I-Gear to operate in Audit mode and, with the AutoAlert feature activated, allow I-Gear to notify you automatically whenever inappropriate accesses have been attempted.

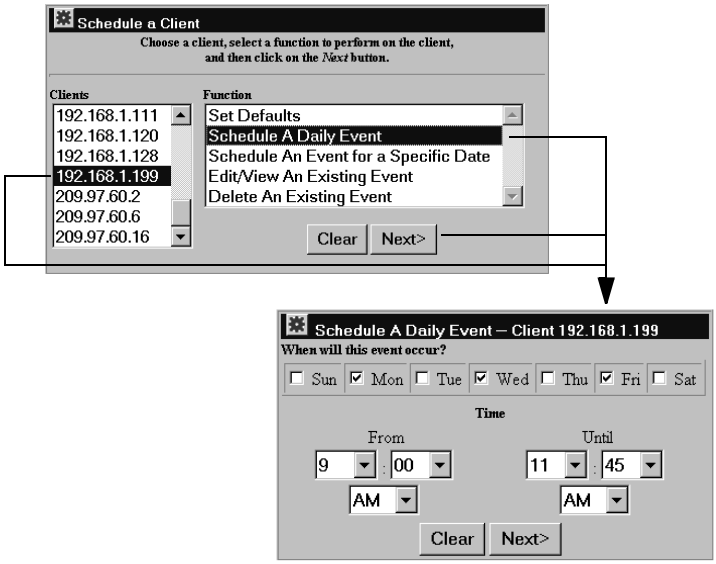
When you have finished setting all filtering options on this display, click the **Finish** button. I-Gear will provide confirmation that your changes have been made. If you click the **Cancel Change** button, no default event will be scheduled for the selected Client.

Scheduling a Daily Event

A daily event can be scheduled to override the default access permissions for an object. Daily events reoccur on the day(s) specified until the event is edited or deleted. For example, you could set a Client, User, or Cast to be locked by default and then schedule a daily event to permit Internet access.

To schedule a daily event for a given Client, select the Client and the Schedule a Daily Event function. Then click the **Next** button.

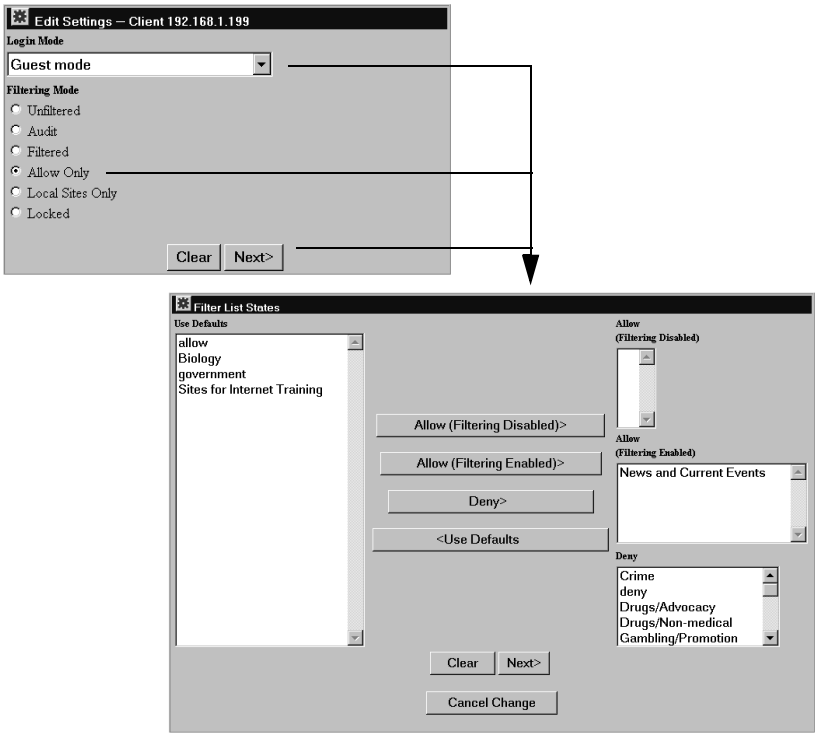
Select the day(s) of the week and the time during which the event will occur. Then click the **Next** button.



Select the appropriate login mode and the filtering permissions for the event, as described in the previous subsection entitled “Set Defaults.” Then click the **Next** button.

If you select Unfiltered, Locked, or Local Sites Only, you will receive confirmation that the event has been scheduled. Click the **Done** button to return to the I-Gear administrative interface.

If you select Filtered, Allow Only, or Audit, you must next select the List states that will apply during the scheduled event. Then click the **Next** button.

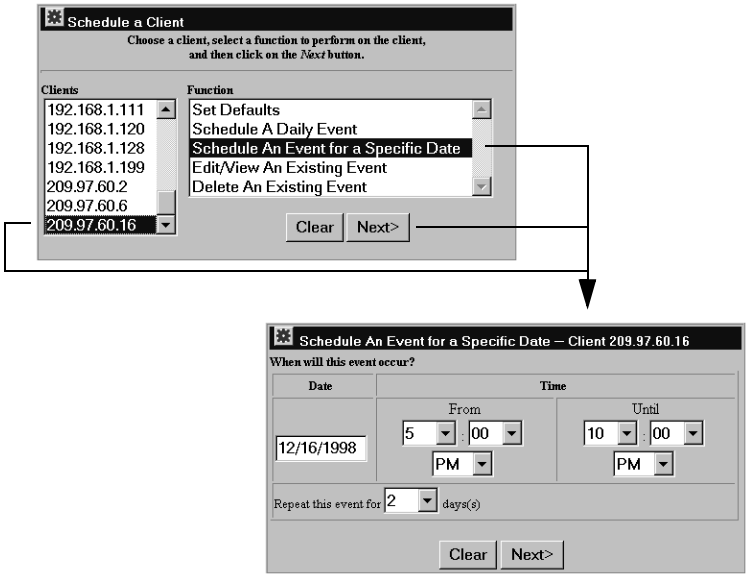


You then will be prompted for other filtering settings. Select the filtering settings that will apply during the event, as discussed previously. Then click the **Finish** button. If you click the **Cancel Change** button, no event will be scheduled.

Note: Remember that a daily event remains in effect indefinitely until the event is deleted.

Scheduling an Event for a Specific Date

To schedule a specific event for a Client, select the Client and the Schedule An Event for a Specific Date function. Then click the **Next** button.



Select the date and time of day for the event and the number of days that the event will repeat. Then click the **Next** button. You may choose to have specific events repeat for up to 14 days. Specific events are automatically deleted when they have concluded.

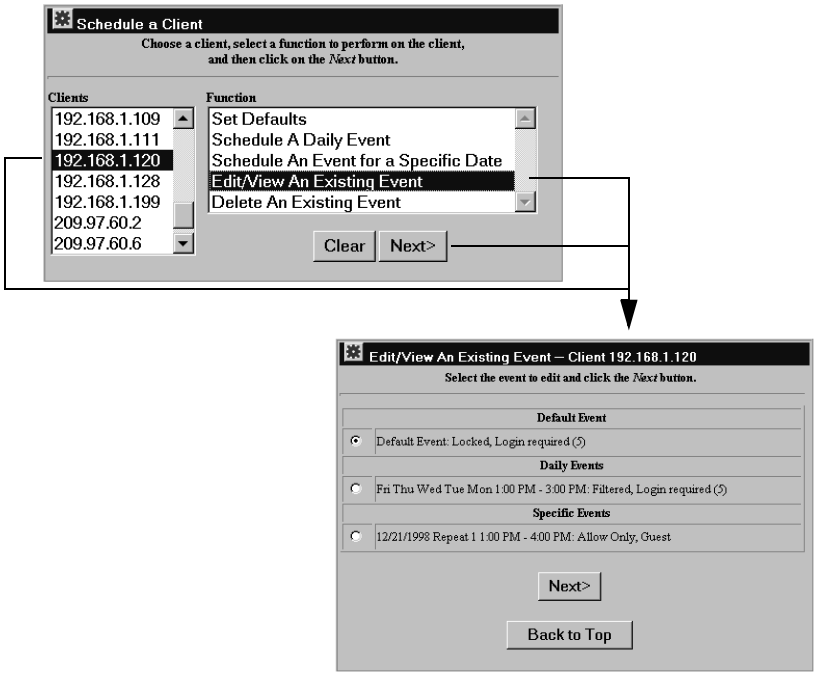
Select the appropriate login mode and the filtering permissions for the event, as described previously in “Setting Defaults” on page 57. Then click the **Next** button.

If you select Unfiltered, Locked, or Local Sites Only, you will receive confirmation that the event has been scheduled. Then click the **Done** button to return to the I-Gear administrative interface.

If you select Filtered, Allow Only, or Audit, you must next select the List states that will apply during the scheduled event. Then click the **Next** button again. You will be prompted for other filtering settings. Select the filtering settings that will apply during the event, as discussed previously. Then click the **Finish** button. If you click the **Cancel Change** button, no event will be scheduled.

Editing an Existing Event

To edit an existing event for a Client, select the Client to which the event applies and the Edit/View an Existing Event function. Then click the **Next** button.


Schedule a Client
Choose a client, select a function to perform on the client, and then click on the Next button.
Clients
192.168.1.109
192.168.1.111
192.168.1.120
192.168.1.128
192.168.1.199
209.97.60.2
209.97.60.6
Function
Set Defaults
Schedule A Daily Event
Schedule An Event for a Specific Date
Edit/View An Existing Event
Delete An Existing Event
Clear
Next>
Edit/View An Existing Event – Client 192.168.1.120
Select the event to edit and click the Next button.
Default Event
Default Event: Locked, Login required (5)
Daily Events
Fri Thu Wed Tue Mon 1:00 PM - 3:00 PM: Filtered, Login required (5)
Specific Events
12/21/1998 Repeat 1 1:00 PM - 4:00 PM: Allow Only, Guest
Next>
Back to Top

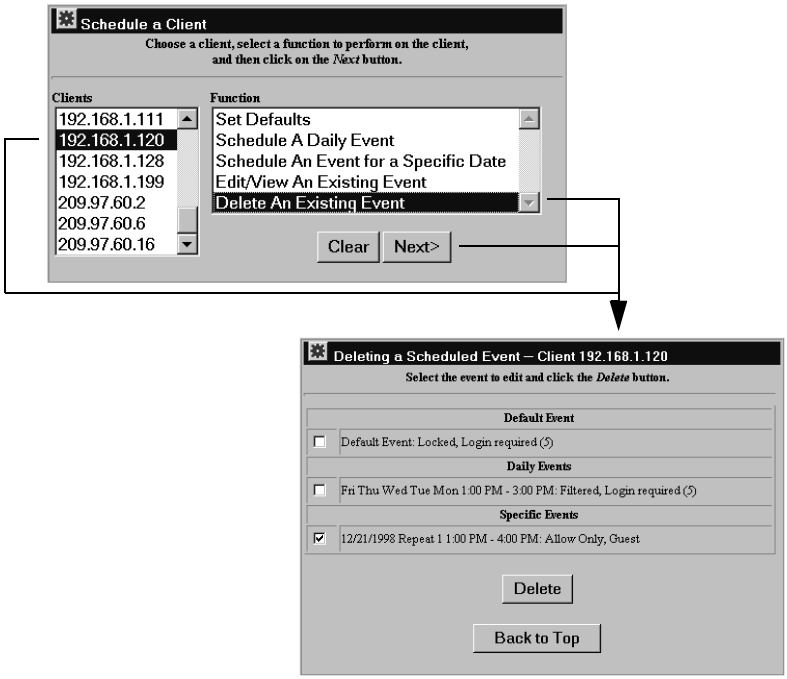
A list of all events that apply to the specified Client is shown. Note that the event with the lowest priority—the default settings for the Client—is shown at the top and that the event(s) with the highest priority—the specific event(s)—are listed at the bottom.

Select the event you wish to modify. Then click the **Next** button. You will be shown appropriate displays for editing the selected event—make the desired changes as described in detail in “Setting Defaults” on page 57.

Note: You cannot change an event from one type to another, for example, from a daily event to a specific event.

Deleting an Existing Event

To delete a scheduled event for a Client, select the Client for which an event is to be deleted and the Delete an Existing Event function. Then click the **Next** button.


Schedule a Client
Choose a client, select a function to perform on the client, and then click on the Next button.
Clients
192.168.1.111
192.168.1.120
192.168.1.128
192.168.1.199
209.97.60.2
209.97.60.6
209.97.60.16
Function
Set Defaults
Schedule A Daily Event
Schedule An Event for a Specific Date
Edit/View An Existing Event
Delete An Existing Event
Clear
Next>
Deleting a Scheduled Event – Client 192.168.1.120
Select the event to edit and click the Delete button.
Default Event
Default Event: Locked, Login required (5)
Daily Events
Fri Thu Wed Tue Mon 1:00 PM - 3:00 PM: Filtered, Login required (5)
Specific Events
12/21/1998 Repeat 1 1:00 PM - 4:00 PM: Allow Only, Guest
Delete
Back to Top

A list of all events that apply to the specified Client will be shown. Select the event(s) to be deleted. Then click the **Finish** button.

Generating a Report for a Client

The Report method is the same for the Client, User, and Cast objects. Two types of reports can be generated for these objects: Access Reports and Access Summary Reports. The Access Report allows you to review the browsing activity (e.g., URLs that were accessed or for which access was attempted, violations) and the administrative activity (e.g., logins, logouts) for the selected object(s). The Access Summary Report provides summary information on frequency of access for popular URLs, the most active Users and Clients, and the frequency and types of violations.

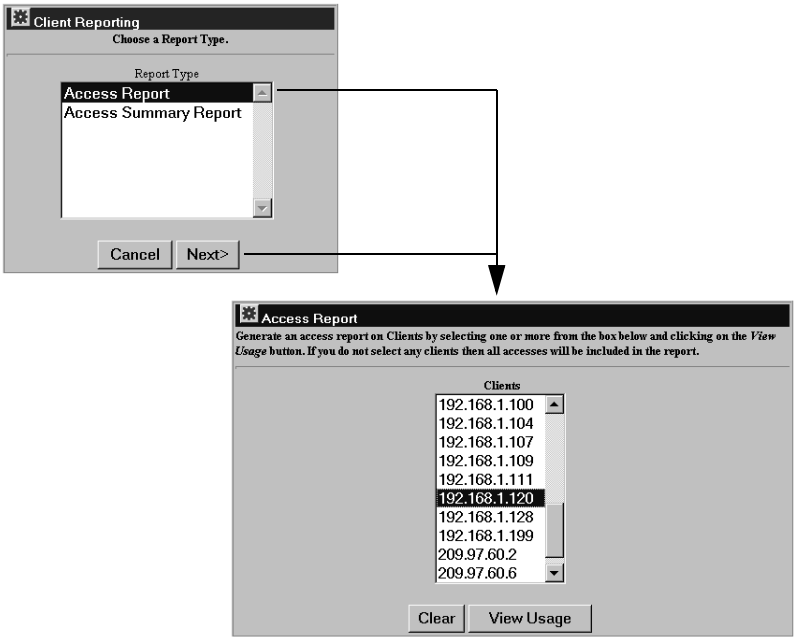
Note: Reporting for a particular Client is dependent both on the settings for the specific Client and the System default settings in regard to the

type of browsing activity that I-Gear is to log. (See “Modifying Other Settings” on page 130 and “Modifying a Client” on page 51 for more information.) For example, if you have elected to have no browsing activity logged for a particular Client, an Access Report generated for that Client will not contain information on browsing activity.

Access Reports

To generate an Access Report for a given Client, click the Report link from the Client administration page or the Client Report shortcut from the main I-Gear administration page. Then select Access Report and click the **Next** button.

Select the IP address(es) of the Client(s) on which you want to report. Then click the **View Usage** button. If no Clients are selected, *all* Clients in the list will be included in the report.



Select the date and the range of time to be covered in the report. Then specify the type of information to be included in the report. If none of the check boxes are selected, then the report will include *all* types of information. If one or more check boxes are selected, the report will

contain only the requested content. The types of information are described in the tables below.

Realms	Description
Administration	Administrative functions performed by Users with administrative privileges will be reported.
I-Gear	All browsing activity for the selected object(s) will be reported.

Actions	Description
Login	All login activity for the selected object(s) will be reported.
Logout	All logout activity for the selected object(s) will be reported.
Content Violation	All Internet access attempts that resulted in a User being blocked will be reported for the selected object(s).
Audit Violation	All Internet access attempts in Audit mode that would have resulted in a User being blocked if the User were actually being filtered will be reported for the selected object(s).
AutoLocked	All activity that resulted in a User being AutoLocked will be reported for the selected object(s).
Access Violation	All attempts to access the I-Gear administration pages by Users who do not have administrative permissions will be reported for the selected object(s).
Object Added	All objects added to I-Gear will be reported for the selected object(s).
Object Deleted	All objects deleted from I-Gear will be reported for the selected object(s).
Object Modified	All modified objects will be reported for the selected object(s).
Object Scheduled	All scheduled objects will be reported for the selected object(s).
Object Renamed	All renamed objects will be reported for the selected object(s).

Actions	Description
File Downloaded	All files automatically downloaded (i.e., filter lists, dictionaries) will be reported.
URL Visited	All URLs visited for the selected object(s) will be reported.
Cache Statistics	All logs for cache statistics will be reported for the time period covered by the Access Report. (Approximately once every minute I-Gear logs the cache statistics for the previous minute.) This information is used to build the Cache Summary Reports. However, if desired, you can view the individual logs generated each minute.

If you want the URLs that appear in the report to be active links to permit easy review, also select the Turn URLs into Links check box.

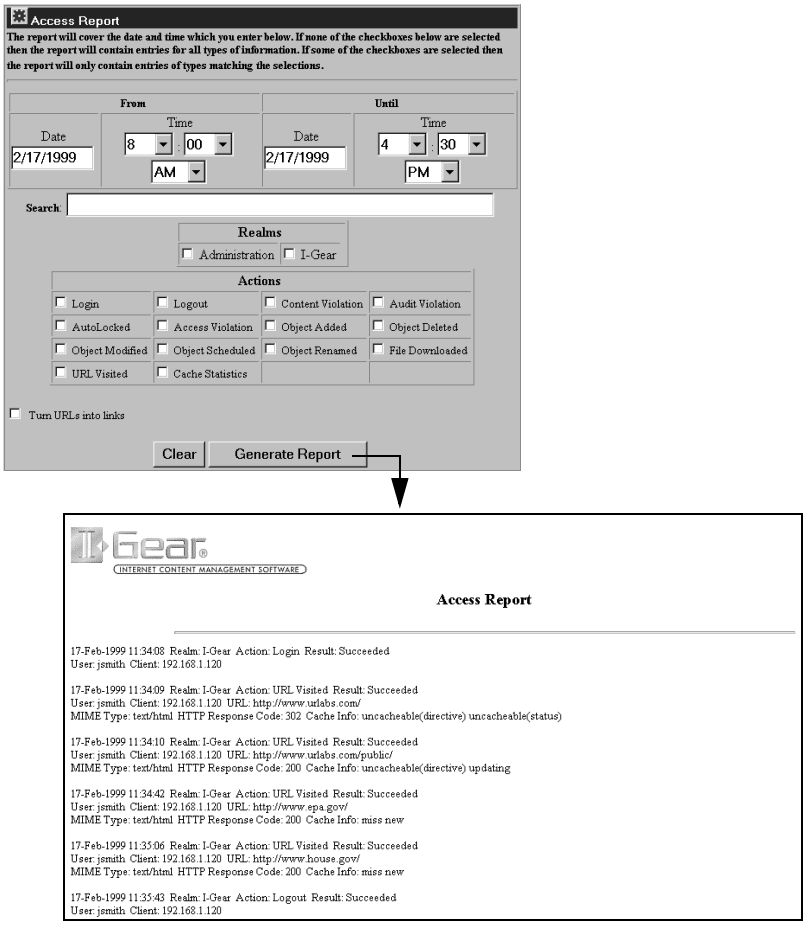
Note: Keep in mind that for larger reports selecting the Turn URLs into Links option may generate too much data for the Web browser to process in a timely manner.

The search field is provided so that you can search for particular text. For example, to see how many Users tried to access a particular site, such as `playboy.com`, simply enter `playboy` in the search field and the report will display any report entries that contain that text.

After you have selected the appropriate check boxes, click the **Generate Report** button. Clicking the **Clear** button will clear the display.

In the Access Report, each access is reported on two to three lines, depending on the amount of data available. The first line contains the date and time the reported action occurred, the realm (e.g., I-Gear, Administration), the action (e.g., login, URL visited, object scheduled, content violation), and the result (e.g., succeeded, failed). The second line indicates the User, the Client from which the action was initiated, and the URL accessed or for which access was attempted (if appropriate). The third line includes the MIME type of information accessed, the HTTP response code, and related cache information (e.g., whether the request was served from the cache, whether the data were cacheable, and so on). Any additional information available on the particular action

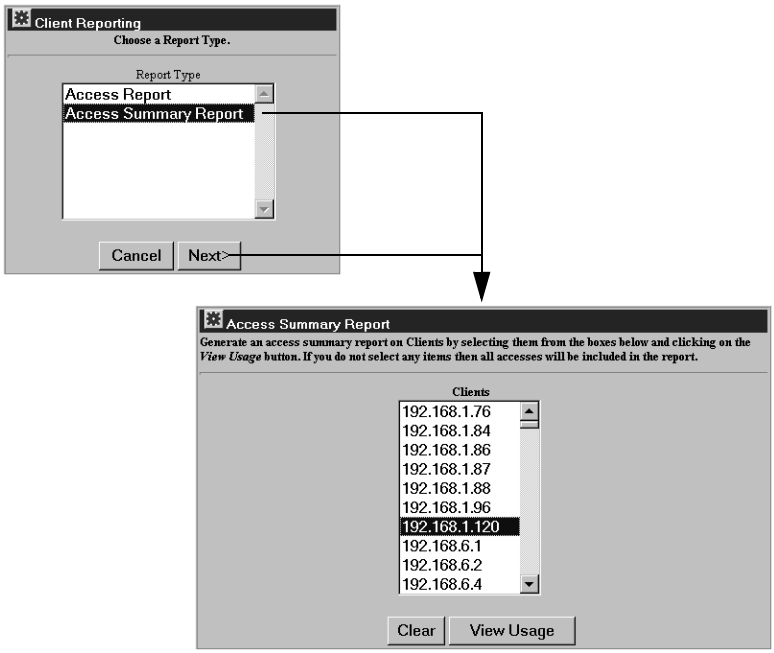
may be included as appropriate (e.g., logoff due to timeout, violation - DDR, and so on).


Access Report
The report will cover the date and time which you enter below. If none of the checkboxes below are selected then the report will contain entries for all types of information. If some of the checkboxes are selected then the report will only contain entries of types matching the selections.
From
Until
Date
Time
2/17/1999
8 : 00 AM
2/17/1999
4 : 30 PM
Search
Realms
Administration
I-Gear
Actions
Login
Logout
Content Violation
Audit Violation
AutoLocked
Access Violation
Object Added
Object Deleted
Object Modified
Object Scheduled
Object Renamed
File Downloaded
URL Visited
Cache Statistics
Turn URLs into links
Clear
Generate Report
INTERNET CONTENT MANAGEMENT SOFTWARE
Access Report
17-Feb-1999 11:34:08 Realm: I-Gear Action: Login Result: Succeeded
User: jsmith Client: 192.168.1.120
17-Feb-1999 11:34:09 Realm: I-Gear Action: URL Visited Result: Succeeded
User: jsmith Client: 192.168.1.120 URL: http://www.urlabs.com/
MIME Type: text/html HTTP Response Code: 302 Cache Info: uncacheable(directive) uncacheable(status)
17-Feb-1999 11:34:10 Realm: I-Gear Action: URL Visited Result: Succeeded
User: jsmith Client: 192.168.1.120 URL: http://www.urlabs.com/public/
MIME Type: text/html HTTP Response Code: 200 Cache Info: uncacheable(directive) updating
17-Feb-1999 11:34:42 Realm: I-Gear Action: URL Visited Result: Succeeded
User: jsmith Client: 192.168.1.120 URL: http://www.epa.gov/
MIME Type: text/html HTTP Response Code: 200 Cache Info: miss new
17-Feb-1999 11:35:06 Realm: I-Gear Action: URL Visited Result: Succeeded
User: jsmith Client: 192.168.1.120 URL: http://www.house.gov/
MIME Type: text/html HTTP Response Code: 200 Cache Info: miss new
17-Feb-1999 11:35:43 Realm: I-Gear Action: Logout Result: Succeeded
User: jsmith Client: 192.168.1.120

Access Summary Reports

To generate an Access Summary Report for a given Client, select the Report link from the Client administration page or the Client Report shortcut from the main I-Gear administration page. Then select Access Summary Report and click the **Next** button.

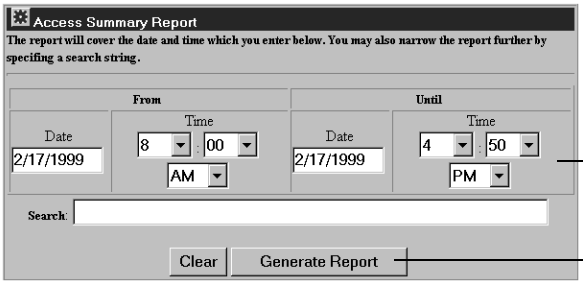
Select the IP address(es) of the Client(s) on which you want to report and click the **View Usage** button. If no Clients are selected, then *all* Clients in the list will be included in the report.

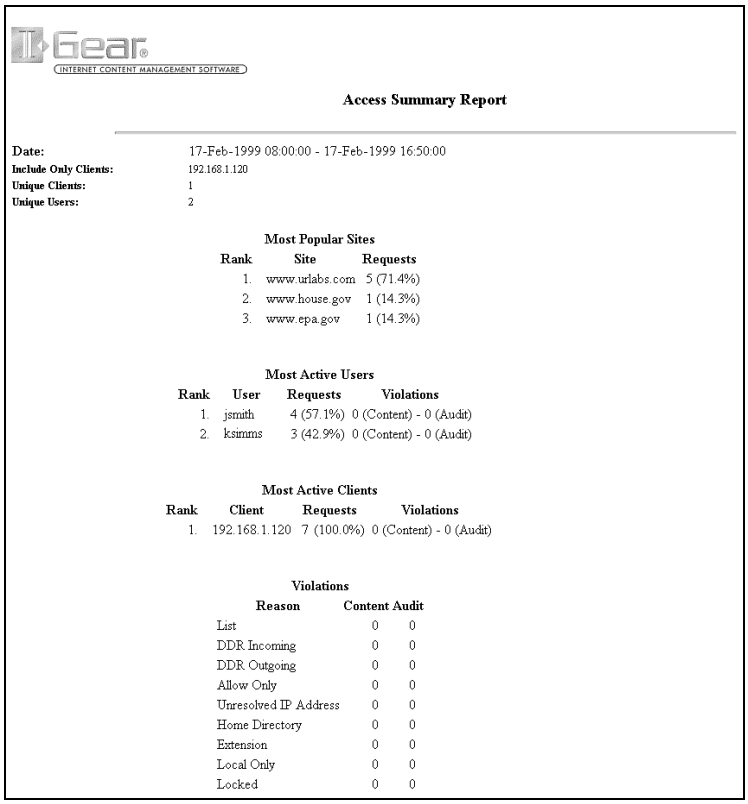


From the next display, select the date and range of time to be covered in the report and click the **Generate Report** button.

The Access Summary Report includes, for the Client(s) selected, the most frequently accessed URLs, the most active Users (who have used

the selected Client(s)), the most active Clients, and a summary of violations from the selected Client(s).





Gear
INTERNET CONTENT MANAGEMENT SOFTWARE

Access Summary Report

Date: 17-Feb-1999 08:00:00 - 17-Feb-1999 16:50:00
Include Only Clients: 192.168.1.120
Unique Clients: 1
Unique Users: 2

Most Popular Sites

Rank	Site	Requests
1.	www.urlabs.com	5 (71.4%)
2.	www.house.gov	1 (14.3%)
3.	www.epa.gov	1 (14.3%)

Most Active Users

Rank	User	Requests	Violations
1.	jsmith	4 (57.1%)	0 (Content) - 0 (Audit)
2.	ksimms	3 (42.9%)	0 (Content) - 0 (Audit)

Most Active Clients

Rank	Client	Requests	Violations
1.	192.168.1.120	7 (100.0%)	0 (Content) - 0 (Audit)

Violations

Reason	Content	Audit
List	0	0
DDR Incoming	0	0
DDR Outgoing	0	0
Allow Only	0	0
Unresolved IP Address	0	0
Home Directory	0	0
Extension	0	0
Local Only	0	0
Locked	0	0

7. Working with the User Object

Adding a User

Users must be added to I-Gear before they can log into I-Gear. Two types of users can be added to I-Gear: System Users and Virtual Users. If a User already has an account on the same domain as the server running I-Gear (or, for Windows NT, any other trusted domain), that account can be automatically added to I-Gear (System User). Virtual Users can also be created in I-Gear. The Virtual User account is only recognized by I-Gear; that is, Virtual User accounts in I-Gear do not have corresponding system accounts. Thus, valuable network resources are not used to maintain numerous system accounts for Users who will be using only I-Gear. Furthermore, Virtual Users do not have access to other parts of the system, which minimizes the security risks that could be associated with larger numbers of system accounts.

If you have purchased the Enterprise version of I-Gear, you also can add RADIUS Users to I-Gear. An I-Gear RADIUS User's password is validated against the User's account on the RADIUS server.

Adding One System User at a Time

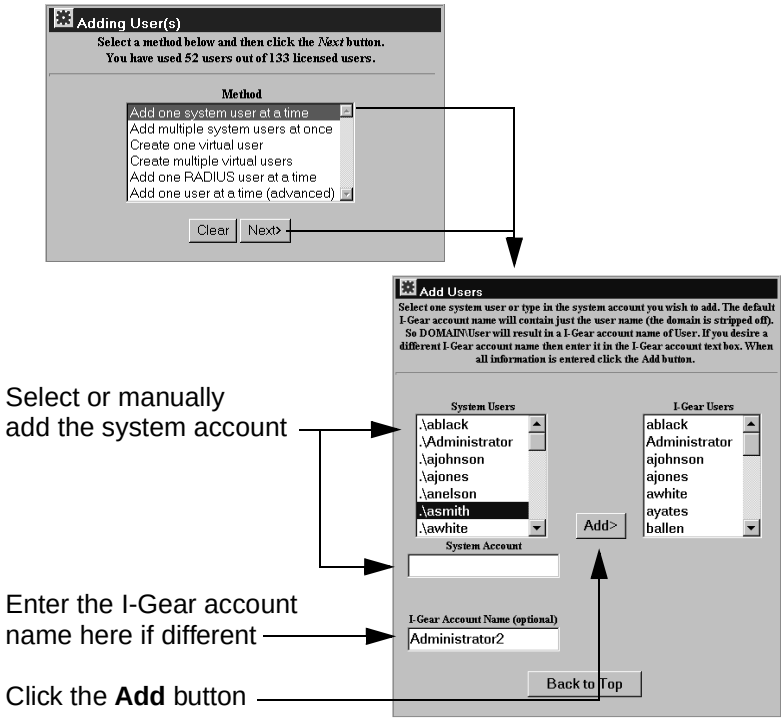
To add a System User to I-Gear, click the Add link from the User object administration page or the User Add shortcut from the main I-Gear administration page. Then select the Add One System User at a Time method, and click the **Next** button.

Current System Users (i.e., system accounts for the same domain as the server running I-Gear and, for Windows NT only, any other trusted domains) are listed on the left side of the display. (Note that domain names are shown in addition to User names if you are using Windows NT.) Select from this list the account to be added to I-Gear, or enter the account name in the System Account field.

Note: For Windows NT, the default I-Gear account name contains only the User name; that is, the domain name is stripped off. For example, if the system account name is `asmith` in `domainA` (i.e., `DomainA\asmith`), the default I-Gear user name is `asmith`.

If you prefer a different name for the I-Gear account, you must enter the desired account name in the space provided. For example, if you (System User `asmith`) wanted your I-Gear account name to be

Administrator2, you would select your system account and then enter Administrator2 in the I-Gear Account Name field.


Adding User(s)
Select a method below and then click the Next button.
You have used 52 users out of 133 licensed users.
Method
Add one system user at a time
Add multiple system users at once
Create one virtual user
Create multiple virtual users
Add one RADIUS user at a time
Add one user at a time (advanced)
Clear
Next>
Add Users
Select one system user or type in the system account you wish to add. The default I-Gear account name will contain just the user name (the domain is stripped off). So DOMAIN\User will result in a I-Gear account name of User. If you desire a different I-Gear account name then enter it in the I-Gear account text box. When all information is entered click the Add button.
System Users
.\ablack
.\Administrator
.\ajohnson
.\ajones
.\anelson
.\asmith
.\awhite
I-Gear Users
ablack
Administrator
ajohnson
ajones
awhite
ayates
ballen
Add>
System Account
I-Gear Account Name (optional)
Administrator2
Back to Top
Select or manually add the system account
Enter the I-Gear account name here if different
Click the Add button

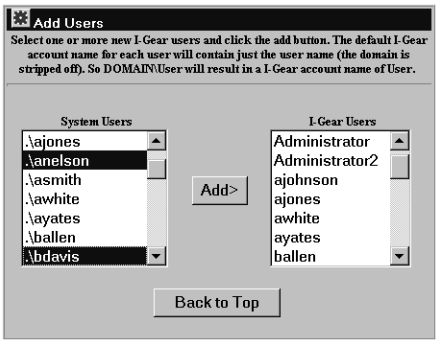
After you have entered the desired information, click the **Add** button. The new I-Gear User account name (in the above example, Administrator2) should appear in the List on the right side of the display. Click the **Back to Top** button when you have finished to return to the main I-Gear administration page.

Note: The password from the system account is the password for the I-Gear account. Users with appropriate permissions who want to change their I-Gear account passwords can do so by clicking the **Password** button on the I-Gear tool bar.

Adding Multiple System Users at Once

To add more than one System User at a time, click the Add link from the User object administration page or the User Add shortcut from the main I-Gear administration page. Then select Add Multiple System Users at Once, and click the **Next** button.

Current System Users (i.e., system accounts for the same domain as the server running I-Gear and, for Windows NT only, any other trusted domains) appear on the left side of the display. (Note that domain names are shown if you are using Windows NT.) Select the System Users you wish to add to I-Gear from the list of User accounts, and click the **Add** button.



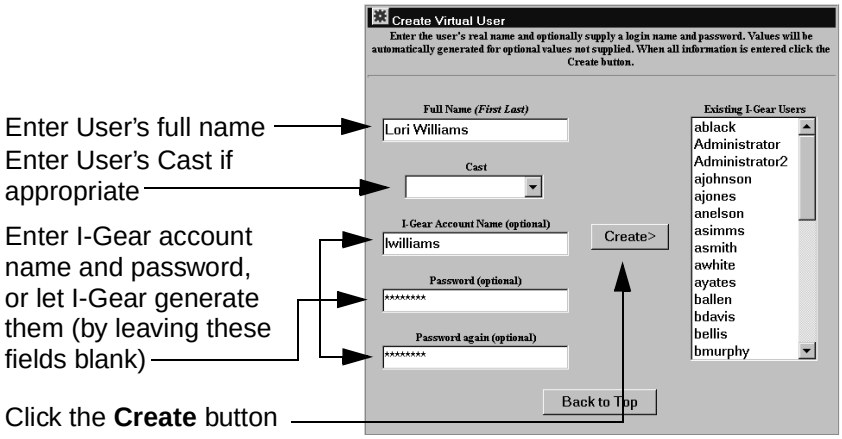
Note: When multiple System Users are added to I-Gear at the same time, the I-Gear account names and passwords are the same as for the system accounts. Users with appropriate permissions who want to change their I-Gear account passwords can do so by clicking the **Password** button on the I-Gear tool bar.

Creating a Single Virtual User

To create one Virtual User, click the Add link from the User administration page or the User Add shortcut from the main I-Gear administration page. Select Create One Virtual User and click the **Next** button. Clicking the **Clear** button will clear the display.

Enter the User's full name in the space provided. Then select a Cast for the User, if appropriate. Optionally, you also can specify an I-Gear login name and password. If you do not specify an account name and password, I-Gear will generate these for you. (Clicking the **Back to Top** button at any time will return you to the I-Gear administration page.) When you have finished entering information on the new account, click the **Create** button. I-Gear will confirm creation of the new Virtual User

account. Click the **Done** button to return to the I-Gear administration page.



Note: If a Virtual User forgets a password, any administrator with the Modify User permission can issue a new password for a Virtual User account using the Modify method for the User object. (The Modify User display for a Virtual User account allows the administrator to enter and verify a new password.) Virtual Users with permission to change their own password can still do so; however, in order to change their own password, Users must know their old password.

Creating Multiple Virtual Users

To add more than one Virtual User at a time, create a file that contains a block of information about each Virtual User you wish to add. In this file, the information for each User must be on a separate line and formatted as follows.

```
Full name,account name,password,cast
```

The full name is mandatory; all other fields are optional. If you do not specify an account name or password, I-Gear will generate these for you. Note that you must type all three commas even if you do not specify any information other than the full name. Examples:

```
Joe Smith,smith,boat,xyz

Jane Smith,,,
```

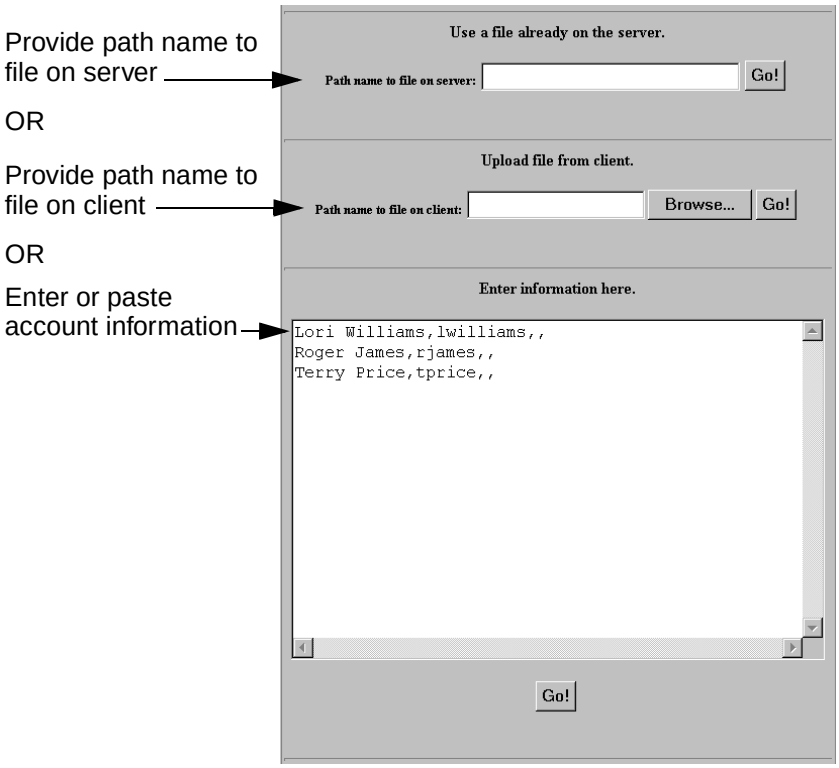
When the file is complete, click the Add link from the User administration page or the User Add shortcut from the main I-Gear administration page. Select Create Multiple Virtual Users and click the **Next** button. Clicking the **Clear** button will clear the display.

You must supply the file to the server in one of three ways.

1. If the file is already located on the server, under Use a File Already on the Server enter the path name of the file in the space provided. Then click the corresponding **Go!** button.

2. If the file is located on the machine you are currently using, under Upload File from Client enter the path name of the file in the space provided and click the corresponding **Go**! button or browse for the file by clicking the **Browse** button. (This option requires a browser capable of file uploads.) When you have identified the file in the browse window, click the **Open** button. Then click the corresponding **Go!** button.

3. Enter or paste the file into the text area provided under "Enter information here." Then click the corresponding **Go!** button.

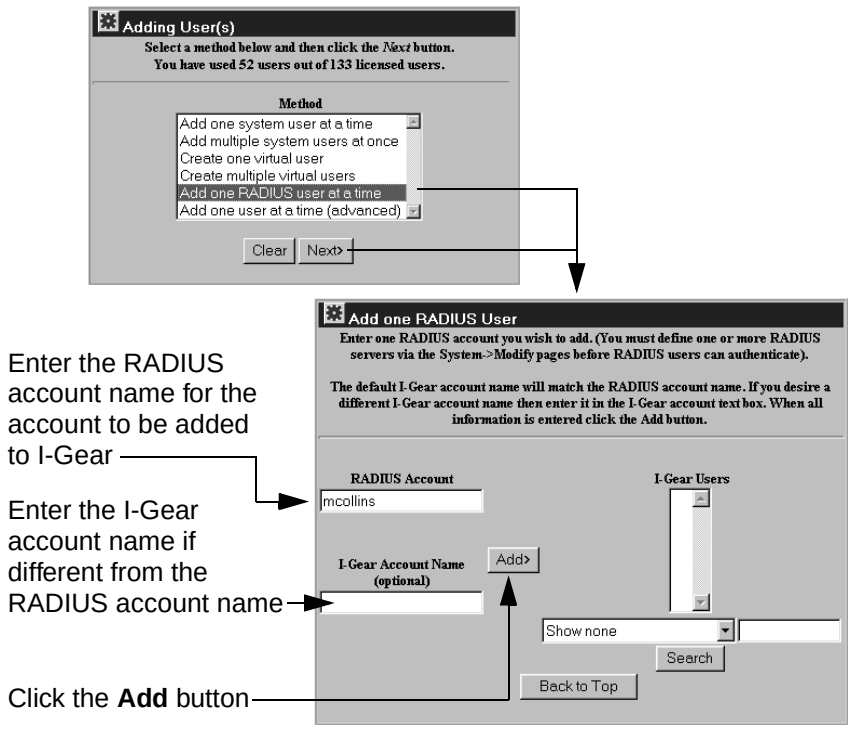


You will receive confirmation that the requested Virtual User accounts have been created. Click the **Done** button to return to the main I-Gear administration page.

Adding One RADIUS User at a Time (Enterprise version only)

If you have purchased the Enterprise version of I-Gear, you will also have the option to add a RADIUS User to I-Gear. To add a RADIUS User, click the Add link from the User object administration page or the User Add shortcut from the main I-Gear administration page. From the next display, select Add One RADIUS User at a Time, and click the **Next** button.

Enter the account name for the RADIUS account that you wish to add to I-Gear in the space provided. If you prefer a different name for the I-Gear account, you must enter the desired account name in the I-Gear Account Name field. If you leave the I-Gear Account Name field blank, the I-Gear account name will be identical to the existing RADIUS account name.


Adding User(s)
Select a method below and then click the Next button.
You have used 52 users out of 133 licensed users.
Method
Add one system user at a time
Add multiple system users at once
Create one virtual user
Create multiple virtual users
Add one RADIUS user at a time
Add one user at a time (advanced)
Clear
Next>
Add one RADIUS User
Enter one RADIUS account you wish to add. (You must define one or more RADIUS servers via the System->Modify pages before RADIUS users can authenticate).
The default I-Gear account name will match the RADIUS account name. If you desire a different I-Gear account name then enter it in the I-Gear account text box. When all information is entered click the Add button.
RADIUS Account
mcollins
I-Gear Users
I-Gear Account Name (optional)
Add>
Show none
Search
Back to Top
Enter the RADIUS account name for the account to be added to I-Gear
Enter the I-Gear account name if different from the RADIUS account name
Click the Add button

After you have entered the desired information, click the **Add** button. The new I-Gear User account name should appear in the List on the right side of the display. Click the **Back to Top** button when you have finished to return to the main I-Gear administration page.

Note: You must define one or more RADIUS servers using the Modify method for the System object before RADIUS users can authenticate.

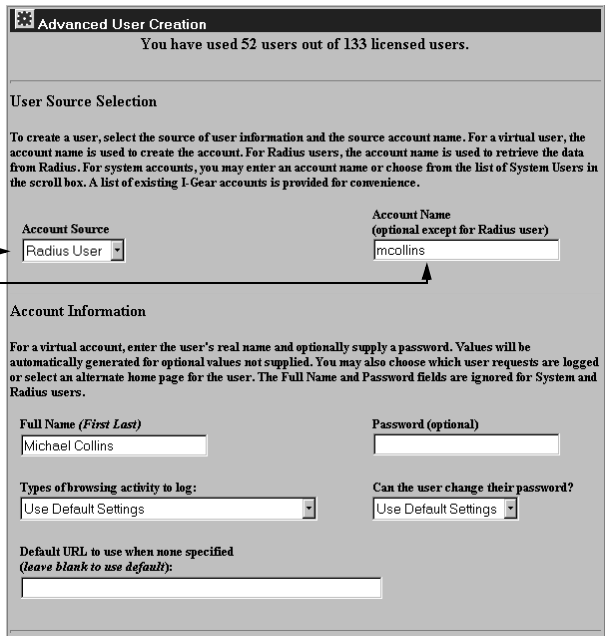
Note: The password from the RADIUS account is the password for the I-Gear account. Users with appropriate permissions who want to change their I-Gear account passwords can do so by clicking the **Password** button on the I-Gear tool bar.

Adding One User at a Time (Advanced)

This shortcut for adding any type of User to I-Gear allows you to assign permissions and set certain parameters for the newly created User (without having to go back and use the Modify method for the User). To use this advanced functionality to add a User, click the Add link from the User object administration page or the User Add shortcut from the main I-Gear administration page. From the next display, select Add One User at a Time (Advanced) from the menu, and click the **Next** button.

Enter the type of User to be added and an account name (if you do not enter an account name for a Virtual User, I-Gear will generate one automatically)

Enter the account information (if you do not enter a password for a Virtual User, I-Gear will generate one automatically)


Advanced User Creation
You have used 52 users out of 133 licensed users.
User Source Selection
To create a user, select the source of user information and the source account name. For a virtual user, the account name is used to create the account. For Radius users, the account name is used to retrieve the data from Radius. For system accounts, you may enter an account name or choose from the list of System Users in the scroll box. A list of existing I-Gear accounts is provided for convenience.
Account Source
Radius User
Account Name
(optional except for Radius user)
mcollins
Account Information
For a virtual account, enter the user's real name and optionally supply a password. Values will be automatically generated for optional values not supplied. You may also choose which user requests are logged or select an alternate home page for the user. The Full Name and Password fields are ignored for System and Radius users.
Full Name (First Last)
Michael Collins
Password (optional)
Types of browsing activity to log:
Use Default Settings
Can the user change their password?
Use Default Settings
Default URL to use when none specified
(leave blank to use default):

From the next display, select the type of account (System, Virtual, or RADIUS User) from the pull-down menu on the left (the RADIUS selection will only appear if you have the Enterprise version of I-Gear). If you are creating a System or RADIUS User, enter the System or RADIUS account name in the field provided on the right side of the display. If you are creating a Virtual User, you do not need to enter an account name. If you do not enter an account name, I-Gear will generate one automatically.

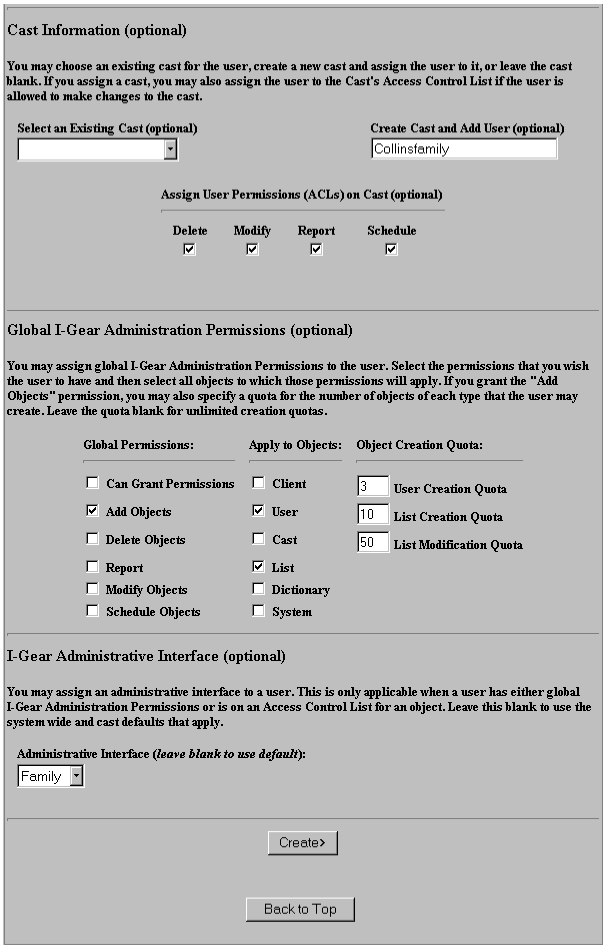
Next, enter the account information. You must enter the User's full name for Virtual Users. If you do not enter a password for a Virtual account, I-Gear will generate one automatically. (For System and RADIUS Users, the I-Gear password will be the same as the corresponding account password.) Next, specify the type of browsing activity to be logged for the User, the default URL that will be displayed when no other URL has been requested, and whether the user can change their password. If you select the Use Default Settings option for any of these settings, other inherited settings will apply based on the hierarchy of permissions.

From the next portion of the display, you can automatically place the User in a Cast if desired. To place the User in an existing Cast, select the Cast from the List of existing Casts on the left side of the display. To create a new Cast for the User, enter the new Cast name in the field provided on the right side of the display. To place the User on the Access Control List for the Cast, select the desired Access Control List permissions for the User by selecting the appropriate check boxes. (The Access Control List permissions check boxes will only display for the Enterprise version of I-Gear.)

Select any global permissions to be granted to the User by selecting the appropriate check boxes under Global I-Gear Administration Permissions. Specify the appropriate quotas for the User (i.e., the total number of Users that can be created, the number of Lists that can be created, and the maximum number of URLs that can be added to Lists by this User) if you have given the User permission to Add Users and Lists.

Note: If you have placed the new User on an Access Control List for a Cast and want the User to be able to create new Users and Lists, you must give the User global Add permissions for the User and List objects.

Finally, select the administrative interface the User will use to perform any administrative functions for which they have permission.

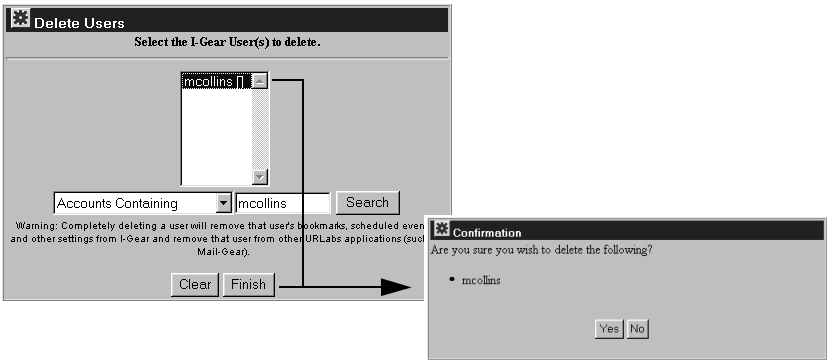

Cast Information (optional)
You may choose an existing cast for the user, create a new cast and assign the user to it, or leave the cast blank. If you assign a cast, you may also assign the user to the Cast's Access Control List if the user is allowed to make changes to the cast.
Select an Existing Cast (optional)
Create Cast and Add User (optional)
Collinsfamily
Assign User Permissions (ACLs) on Cast (optional)
Delete
Modify
Report
Schedule
Global I-Gear Administration Permissions (optional)
You may assign global I-Gear Administration Permissions to the user. Select the permissions that you wish the user to have and then select all objects to which those permissions will apply. If you grant the "Add Objects" permission, you may also specify a quota for the number of objects of each type that the user may create. Leave the quota blank for unlimited creation quotas.
Global Permissions:
Can Grant Permissions
Add Objects
Delete Objects
Report
Modify Objects
Schedule Objects
Apply to Objects:
Client
User
Cast
List
Dictionary
System
Object Creation Quota:
3
User Creation Quota
10
List Creation Quota
50
List Modification Quota
I-Gear Administrative Interface (optional)
You may assign an administrative interface to a user. This is only applicable when a user has either global I-Gear Administration Permissions or is on an Access Control List for an object. Leave this blank to use the system wide and cast defaults that apply.
Administrative Interface (leave blank to use default):
Family
Create>
Back to Top

When you have finished entering the necessary information, click the **Create** button. I-Gear will confirm that your changes have been made successfully.

Deleting a User

To delete a User from I-Gear, click the Delete link from the User administration page or the User Delete shortcut from the main I-Gear administration page.

Select one or more Users to completely delete from I-Gear, and then click the **Finish** button. I-Gear will ask for confirmation that you want to delete the selected User(s). Click the **Yes** or **No** button as appropriate. I-Gear will provide confirmation that your changes have been made successfully.



Note: Deleting a User permanently removes that User's bookmarks, scheduled events, and other settings from I-Gear and also deletes that User from other URLabs applications installed on that machine.

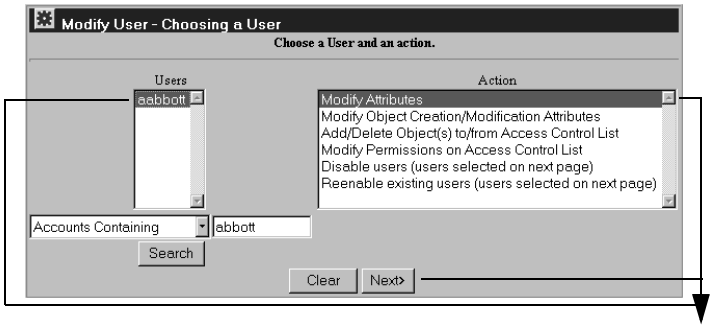
Modifying a User

The Modify method for the User object allows you to assign Users to Casts, select the type of activity to log for individual Users, and grant appropriate I-Gear administrative permissions to Users. (Note that you must have the Can Grant Permissions permission to view and set the permissions of other Users.) You can also change the password for a Virtual User account using the Modify method for the User object.

To modify a User, click the Modify link from the User object administration page or the User Modify shortcut from the main I-Gear administration page.

Modifying Attributes

Select the User to be modified from the left side of the display. Select the Modify Attributes action from the menu on the right side of the display, and click the **Next** button.



Select a Cast for the User (if you want to place the User in a Cast), and specify whether this User can grant Unfiltered (or Audit Mode) access to another User at any time (with the appropriate permissions).

Specify whether the User can change their own password.

Select the type of browsing activity that will be logged for the User, and specify whether the User's browsing history should be retained. Select the appropriate type of logging activity from the pull-down menu, and specify Yes or No for whether the User's history should be retained.

Warning: Many of the Report functions will not operate if activity logging is disabled.

Specify the default URL to display for the User when no other URL has been requested (i.e., the URL that the browser will display automatically after the User clicks the **Login** button).

Note: For the above selections, if you retain the Use Default Settings option, other inherited settings that have been established will apply, based on the hierarchy of permissions.

If the account being modified is a Virtual account, this display will allow you to set a new password, if necessary, for the account. (The new password fields will only appear if the account is a Virtual account.) Thus, if a Virtual User forgets a password, any administrator with the Modify User permission can set a new password for a Virtual User

account from this display. If you want to set a new password, enter the new password twice in the fields provided.

Note: Virtual Users with permission to change their own password can still do so; however, in order to change their own password, Users must know their old password.

Note: For System Users who have system accounts rather than just Virtual accounts with I-Gear, passwords should be modified at the system level rather than through I-Gear.

Then select the appropriate check boxes to change the global administrative permissions for the User. The following table describes each permission that may be granted selectively to User objects.

Permission	Description
Can Grant Permissions	User can grant or change permissions of other Users
Add Objects	User can use the Add method on objects
Delete Objects	User can use the Delete method on objects
Report	User can use the Report method on objects
Modify Objects	User can use the Modify method on objects
Schedule Objects	User can use the Schedule method on objects

Next, select the specific objects (e.g., Client, User) to which the selected permissions apply.

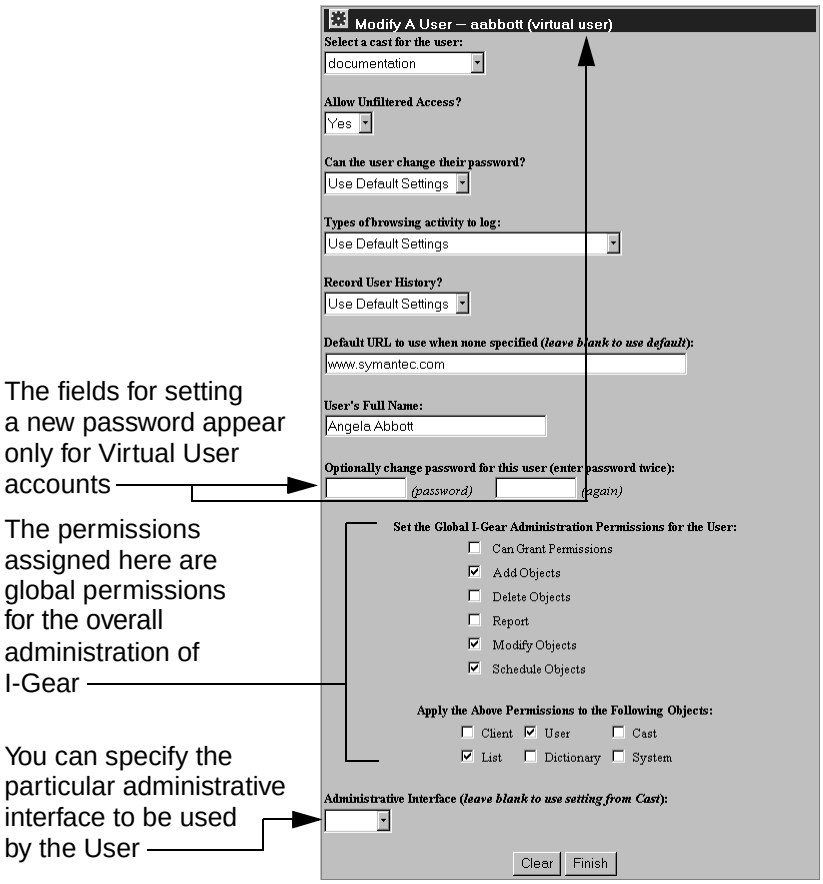
Note: If you have placed the selected User on an Access Control List and want the User to be able to create new Users and private Lists for that Cast, you must give the User global Add permissions for the User and List objects, in addition to the User's Access Control List permissions.

Finally, if you have granted any administrative permissions to the selected User, specify the administrative interface to be used by the User. If the User has not been granted any administrative privileges, this setting is not applicable.

When you have made all appropriate selections, click the **Finish** button. I-Gear will provide confirmation that your changes have been made suc-

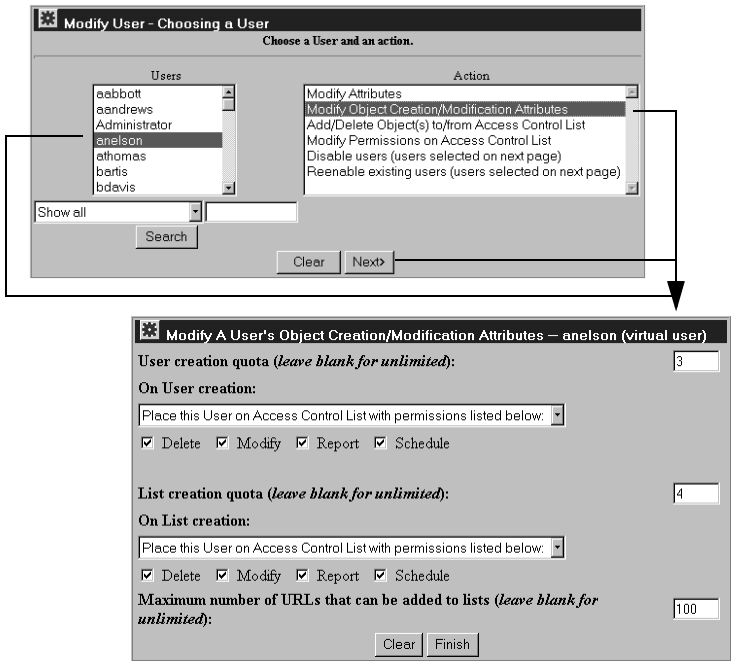
cessfully. Click the **Done** button to return to the main I-Gear administration page.

Note: You cannot change the permissions on your own account. Instead, you must use another account with the Can Grant Permissions permission.


Modify A User – aabbott (virtual user)
Select a cast for the user:
documentation
Allow Unfiltered Access?
Yes
Can the user change their password?
Use Default Settings
Types of browsing activity to log:
Use Default Settings
Record User History?
Use Default Settings
Default URL to use when none specified (leave blank to use default):
www.symantec.com
User's Full Name:
Angela Abbott
Optionally change password for this user (enter password twice):
(password)
(again)
Set the Global I-Gear Administration Permissions for the User:
Can Grant Permissions
Add Objects
Delete Objects
Report
Modify Objects
Schedule Objects
Apply the Above Permissions to the Following Objects:
Client
User
Cast
List
Dictionary
System
Administrative Interface (leave blank to use setting from Cast):
Clear
Finish
The fields for setting a new password appear only for Virtual User accounts
The permissions assigned here are global permissions for the overall administration of I-Gear
You can specify the particular administrative interface to be used by the User

Modifying Object Creation/Modification Attributes

Select the User to be modified from the left side of the display. Select Modify Object Creation/Modification Attributes from the menu on the right side of the display, and click the Next button.



Note: In order to modify the object creation/modification attributes for a User, the selected User must have global permissions for Adding Users and Lists. See the section entitled “Modifying Attributes” on page 89 for information on granting these permissions to Users.

From the next display, specify the number of Users the selected User is allowed to create. Leaving this field blank will allow the User to create an unlimited number of Users.

Next indicate whether the selected User automatically should be placed on the Access Control List for accounts created by the selected User. If you choose to add the selected User to the Access Control List, select the Access Control permissions that should be granted. (The choice to add the User to the Access Control List and the Access Control List permissions check boxes will only display if you have the Enterprise version of I-Gear.)

Specify the number of Lists the selected User is allowed to create. Leaving this field blank will allow the User to create an unlimited number of Lists.

Next indicate whether the selected User should be placed on the Access Control List for new Lists created by the selected User. If you choose to add the selected User to the Access Control List, select the Access Control permissions that should be granted. (The choice to add the User to the Access Control List and the Access Control List permissions check boxes will only display if you have the Enterprise version of I-Gear.)

Enter the maximum number of URLs that can be added to Lists created by this User. Leaving this field blank will allow the User to add an unlimited number of URLs to new Lists.

When you have made the necessary changes, click the **Finish** button. I-Gear will confirm that your changes have been made successfully.

Adding/Deleting Object(s) to/from Access Control List

Adding objects to and deleting objects from Access Control Lists is the same for the Client, User, Cast, and List objects. Refer to “Adding/ Deleting Objects to/from the Access Control List (Enterprise version only)” on page 53 for detailed procedures on adding objects to and deleting objects from Access Control Lists.

Modifying Permissions on Access Control List

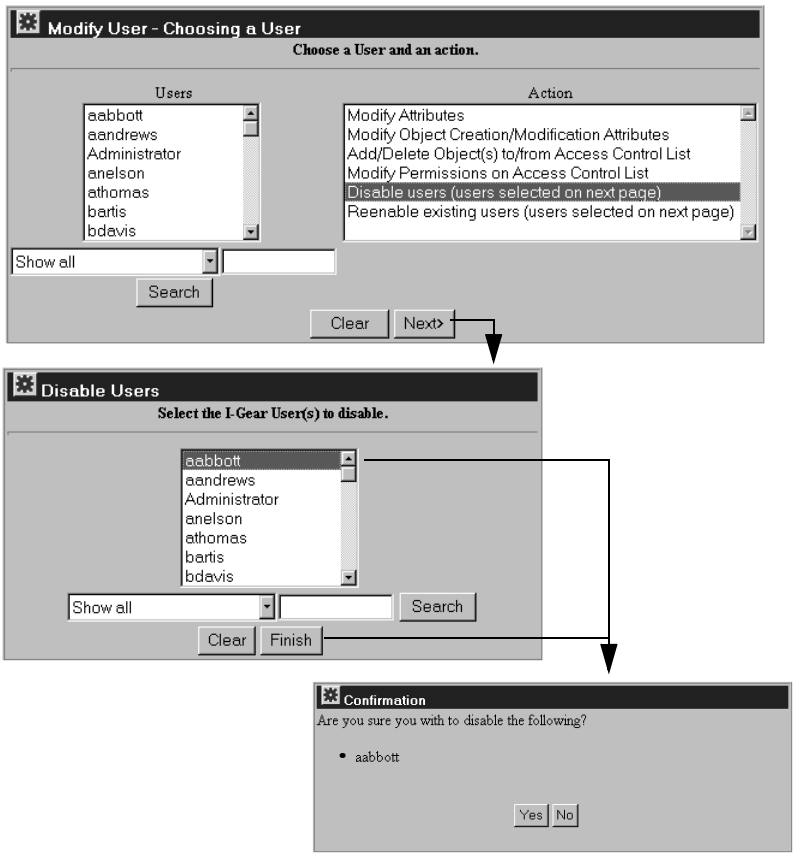
Modifying the permissions for objects on Access Control Lists is the same for the Client, User, Cast, and List objects. Refer to “Modifying Permissions on Access Control List (Enterprise version only)” on page 55 for detailed procedures on modifying the permissions for objects on Access Control Lists.

Disabling Existing Users

To disable existing User(s), select Disable Users from the menu provided, and click the **Next** button.

A list of active User accounts appears on the next display. Select the User(s) you want to disable from the list of User accounts, and click the

Finish button. I-Gear will ask for confirmation that you want to disable the selected User(s). Click the **Yes** or **No** button as appropriate.



Note: An existing User whose account has been disabled will be unable to log on to I-Gear.

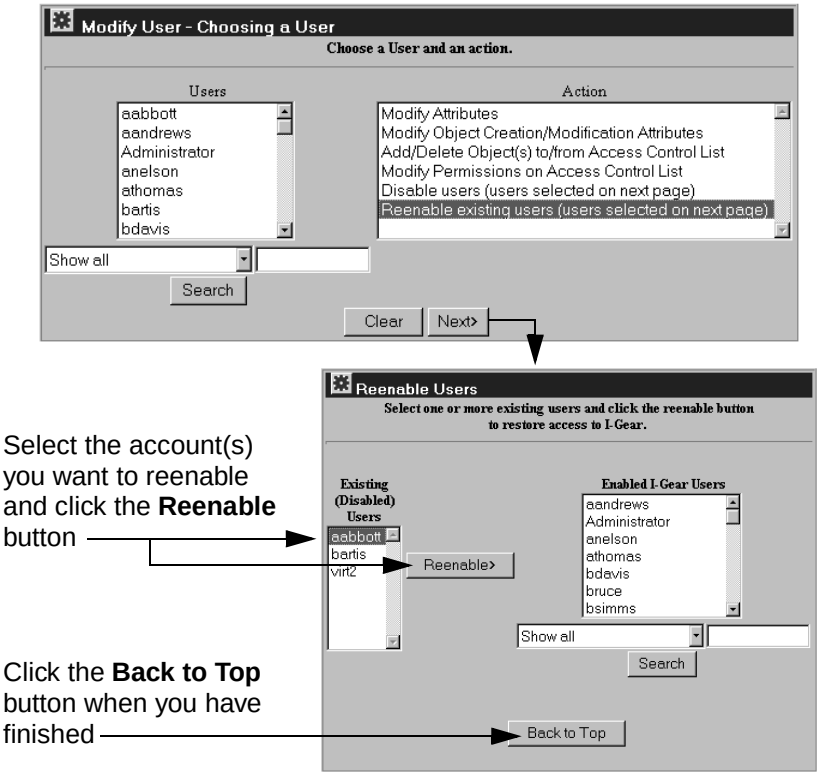
Note: Disabling a User retains the User's bookmarks, scheduled events, and other settings in I-Gear but prevents the User from being able to log on to I-Gear. This option can be used as needed to prevent a User from having any Internet access. If you are running any other URLabs products (e.g., Mail-Gear) on the same machine as I-Gear and are taking advantage of the information-sharing capability between the products, disabling a User from I-Gear will not affect the settings in any other URLabs product.

Reenabling Existing Users

To reenable User accounts that have been disabled, select Reenable Existing Users, and click the **Next** button.

Note: An existing User whose account has been disabled will be unable to log on to I-Gear.

Existing User accounts that have been disabled appear on the left side of the next display. Select the User(s) you want to reenable from the list of User accounts, and click the **Reenable** button. The reenabled Users should then appear in the list on the right side of the display. When you have finished, click the **Back to Top** button.



Scheduling an Event for a User

The Schedule method is the same for Client, User, Cast, and System objects. Refer to the section entitled “Scheduling an Event for a Client” on page 56 for detailed procedures on scheduling events. Remember

that User permissions travel with Users regardless of the machine they use on the network. (However, as noted below, User permissions can be affected, depending on the settings for the Client machine used.)

Note: Keep in mind when scheduling events for Users that by default Client and Client Cast permissions are assigned a higher priority. (See "The I-Gear Design" on page 3 for a discussion on the hierarchy of permissions.) Thus, an event scheduled for a User may be affected by permissions that have been set for a particular Client or Cast of Clients.

Generating a Report for a User

The Report method is the same for the Client, User, and Cast objects for both Access and Access Summary reporting. Refer to "Generating a Report for a Client" on page 71 for detailed procedures on generating these types of reports.

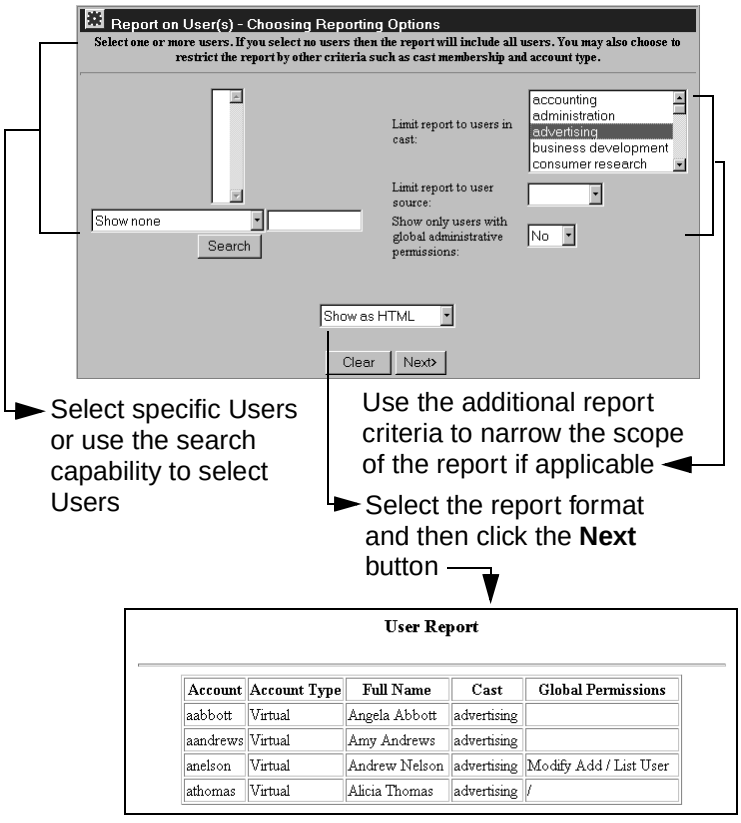
User Summary Reports

The Report method for the User object enables you to review account information for the selected User(s), including the account name, account type, User's full name, User's Cast, and any global permissions that have been granted to the User. To generate a User Summary report, click the Report link from the User administration page or the User Report shortcut from the main I-Gear administration page. From the next display, select User Summary Report from the menu, and click the **Next** button.

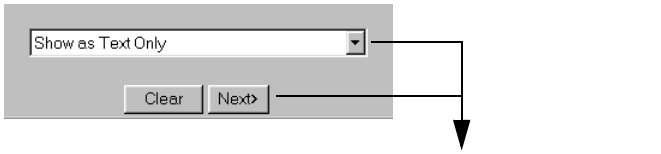
Select the User(s) on which to report from the list shown on the left side of the display. Other criteria are also available to narrow the scope of a report. The pull-down menus on the right side of the display allow you to specify a particular Cast membership on which to report, or you can specify a type of User account on which to report (i.e., virtual, system, or RADIUS accounts). You also can elect to report on only those Users with global administrative permissions if necessary. These criteria work in conjunction with one another to further narrow the scope of the report. For example, if you select the Marketing Cast and select Virtual as the account type, then the report will contain information on only those members of the Marketing Cast who are Virtual Users. For this same example, if you also choose to report on Users who have administrative permissions, then the report would contain information on only those members of the Marketing Cast who have administrative permissions and are also Virtual Users.

Then select whether you want to display the report in HTML or as plain text. If you select Show as Text Only, report results are formatted so that you can save the report output to a file. If you select HTML format, the requested User information is provided in a standard I-Gear HTML report display.

When you have selected the report options, click the **Next** button. The requested information will display in the appropriate report format.



The following example shows the same report generated as text only.




```
User Report
aabbott,Virtual,Angela Abbott,advertising,
aandrews,Virtual,Amy Andrews,advertising,
anelson,Virtual,Andrew Nelson,advertising,Modify Add / List User
athomas,Virtual,Alicia Thomas,advertising,/
```

This report contains the same information as is contained in the HTML report but in text-only format

8. Working with the Cast Object

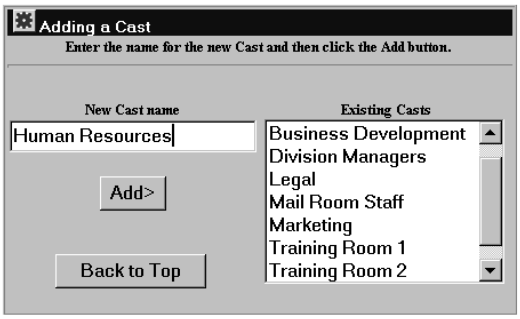
Casting of Client and User objects is a powerful feature of I-Gear. By wisely using System and Cast settings, you can minimize your administrative work. The following rules should guide you in setting up Casts.

- Casts should contain like objects when possible (i.e., Users and Clients should not be mixed in the same Cast).
- Casts should be created when you want to give a group of Users or Clients a different default behavior (e.g., filtering properties). For example, to give certain employees less restrictive Internet access after work hours and on weekends, you could create a Cast that contains these Users. Then scheduling a single daily event for the entire Cast is much more efficient than scheduling the same event for each User individually.
- Casts should be created when a group of Users or Clients will need different permissions during specific times. For example, employee accounts can be locked by default and scheduled to be active every day from 8:00 AM to 5:00 PM.
- Casts for Clients should be based on geographic location (e.g., room 143) or logical group (e.g., teacher computers, summer employees).

If an object is a member of a Cast and you wish to change the object's permissions, scheduling the object will override the Cast permissions. For example, a special student may have his Internet access time extended to 5:00 PM even though he belongs to a Cast for which access is denied after 4:00 PM.

Adding a Cast

To add a Cast to I-Gear, click the Add link from the Cast object administration page or the Cast Add shortcut from the main I-Gear administration page.



Enter the name of the new Cast in the field provided, and click the **Add** button. When you have finished adding new Casts, click the **Back to Top** button to return to the main I-Gear administrative page.

Deleting a Cast

To delete a Cast, click the Delete link from the Cast administration page or the Cast Delete shortcut from the main I-Gear administration page.

Select one or more Cast objects to delete, and click the **Finish** button. More than one Cast can be selected at a time, usually by holding down the control key while selecting the desired Casts—the exact method to select more than one item is browser and operating-system dependent. Clicking the **Clear** button will clear the display. I-Gear will confirm that your changes have been made.

Note: Deleting a Cast will place all members of that Cast into a state of not belonging to any Cast.

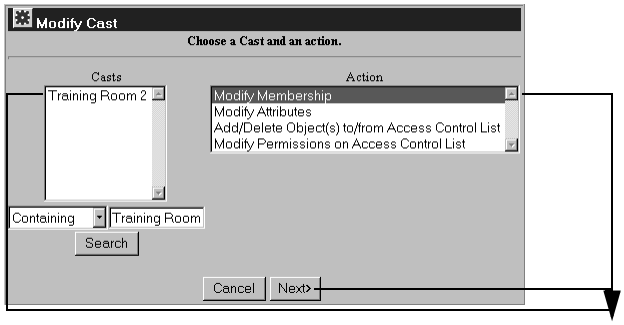
Modifying a Cast

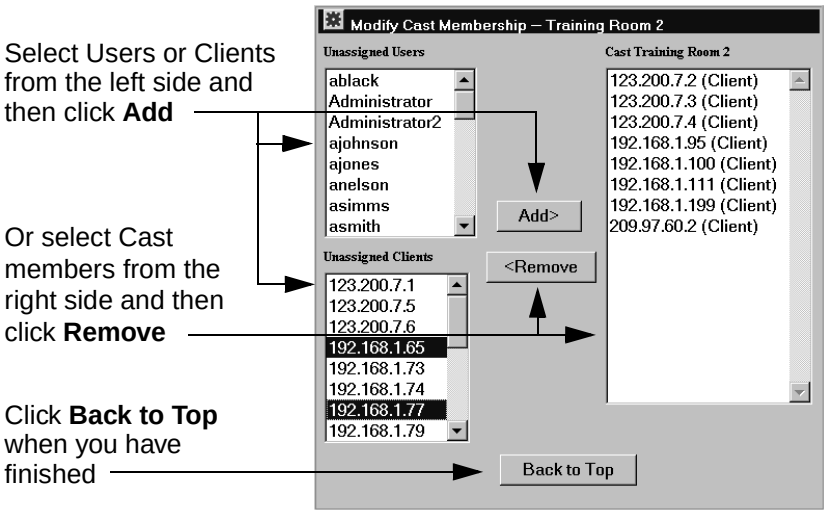
The Modify method for a Cast object allows you to modify the membership or the attributes of existing Casts and modify the Access Control List membership and permissions.

To modify a Cast, click the Modify link from the Cast object administration page or the Cast Modify shortcut from the main I-Gear administration page.

Modifying Cast Membership

To Modify the membership of a Cast, select the Cast to be modified, select Modify Membership from the action menu, and click the **Next** button.





To add objects to the Cast, select one or more unassigned Users or Clients from the left side of the display. Then click the **Add** button. To remove objects from the Cast, select one or more objects from the right side of the display. Then click the **Remove** button. (Objects removed from the Cast will become unassigned.)

Note: Objects can belong to only one Cast at a time. Only those objects not currently assigned to a Cast are displayed in the Unassigned fields on the left.

Modifying Attributes

To modify the attributes for a Cast, select the Cast to be modified, select Modify Attributes from the action menu, and click the **Next** button.

From the next display, first set the permission for whether Cast members can change their password. If you select Use Default Settings, other inherited default settings will apply, subject to the hierarchy of permissions.

Select the type of browsing activity that will be logged for the Cast. If you select Use Default Settings, other inherited default settings will apply, subject to the hierarchy of permissions.

Warning: Many of the Report functions will not operate if activity logging is disabled.

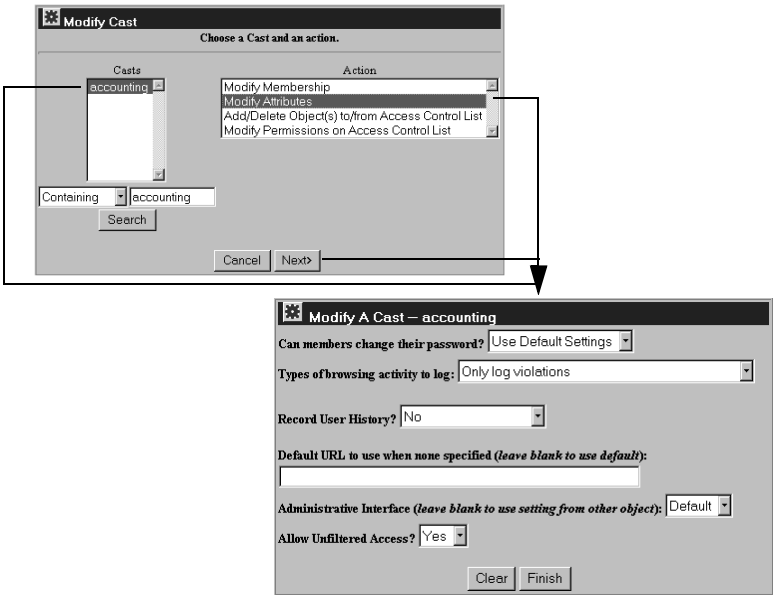
Specify whether browsing history should be recorded for members of the selected Cast. If you select Use Default Settings, other inherited default settings apply, subject to the hierarchy of permissions.

Specify the default URL to display for the Cast when no other URL has been requested (i.e., the URL that the browser will display automatically after a User clicks the **Login** button). If you select Use Default Settings, other inherited default settings apply, subject to the hierarchy of permissions.

Specify the administrative interface that will be displayed for those Cast members who have administrative permissions. If Use Default Settings is selected, other inherited default settings apply, subject to the hierarchy of permissions. (This selection will only appear if you have the Enterprise version of I-Gear.)

Specify whether unfiltered (and Audit Mode) access can be granted by members of the selected Cast. If Use Default Settings is selected, other inherited default settings apply, subject to the hierarchy of permissions.

When you have made the necessary changes, click the **Finish** button. I-Gear will confirm that your changes have been made successfully.



Adding/Deleting Object(s) to/from Access Control List

Adding objects to and deleting objects from Access Control Lists is the same for the Client, User, Cast, and List objects. Refer to “Adding/ Deleting Objects to/from the Access Control List (Enterprise version only)” on page 53 for detailed procedures on adding objects to and deleting objects from Access Control Lists.

Modifying Permissions on Access Control List

Modifying the permissions for objects on Access Control Lists is the same for the Client, User, Cast, and List objects. Refer to “Modifying Permissions on Access Control List (Enterprise version only)” on page 55 for detailed procedures on modifying the permissions for objects on Access Control Lists.

Scheduling an Event for a Cast

The Schedule method is the same for Client, User, Cast, and System objects. Refer to “Scheduling an Event for a Client” on page 56 for detailed procedures on scheduling events.

Note: As you schedule events for Casts, keep in mind the hierarchy of object permissions. The permissions for individual Clients or Users have priority over those for the Cast in which the User or Client is a member. Client and Client Cast permissions have priority over User and User Cast permissions. For example, you could set the default settings for a Cast containing all Clients in the main public area of a library to be in Guest Mode with Filtered access and to not allow files with the .exe extension to be downloaded. You could still allow library patrons to download .exe files from one machine (e.g., a machine located near the front desk) by scheduling an event for the individual Client machine.

Generating a Report for a Cast

The Report method is the same for the Client, User, and Cast objects for both Access and Access Summary reporting. More detailed procedures for generating reports are provided in “Generating a Report for a Client” on page 71.

9. Working with the List Object

Two types of Lists exist in I-Gear: predefined Content Category Lists, which are provided by URLabs, and local Lists, which you create as needed for specific uses. In addition, two versions of each predefined Content Category List exist in I-Gear: a local version and the version populated by URLabs. The local version of each List is provided so that you can add additional related URLs to the Content Category Lists as needed.

Lists can also be made either public or private. A public list is available for use by all objects. A private List can be used only by the Cast members to which the List has been assigned.

Adding a List

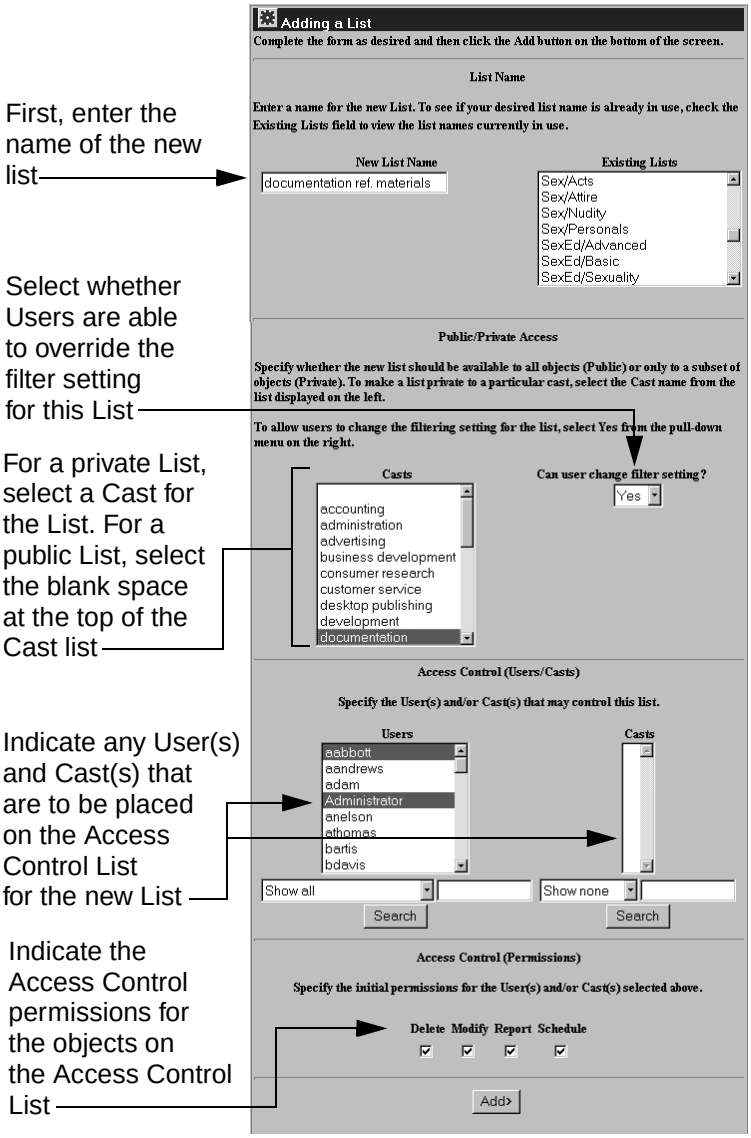
To add a new List to I-Gear, click the Add link from the List object administration page or the List Add shortcut from the main I-Gear administration page.

On the next display, first enter the name of the new List. No two lists can have the same name. (If necessary, you can check the field on the right side of the display to see whether the name you have entered is already in use.)

From the next portion of the display, indicate whether the new List should be private or public. To make the List public, select the blank space at the top of the list of Casts (or do not highlight any entry in the list of Casts). To make the List private, select the Cast to which this new List will be restricted. (Note that only one Cast may be selected for a given List.) Also indicate whether the filtering state of the List can be overridden by Users (by scheduling an event for a User or Cast). This restriction will not apply to Users who have Schedule permission for the System object.

On the next portion of the display, highlight any User(s) and Cast(s) that should be placed on the Access Control List for the new List, and indi-

cate the permissions to be granted to those objects on the Access Control List by clicking the appropriate check boxes.


First, enter the name of the new list
Select whether Users are able to override the filter setting for this List
For a private List, select a Cast for the List. For a public List, select the blank space at the top of the Cast list
Indicate any User(s) and Cast(s) that are to be placed on the Access Control List for the new List
Indicate the Access Control permissions for the objects on the Access Control List
Adding a List
Complete the form as desired and then click the Add button on the bottom of the screen.
List Name
Enter a name for the new List. To see if your desired list name is already in use, check the Existing Lists field to view the list names currently in use.
New List Name
documentation ref. materials
Existing Lists
Sex/Acts
Sex/Attire
Sex/Nudity
Sex/Personals
SexEd/Advanced
SexEd/Basic
SexEd/Sexuality
Public/Private Access
Specify whether the new list should be available to all objects (Public) or only to a subset of objects (Private). To make a list private to a particular cast, select the Cast name from the list displayed on the left.
To allow users to change the filtering setting for the list, select Yes from the pull-down menu on the right.
Casts
Can user change filter setting?
Yes
accounting
administration
advertising
business development
consumer research
customer service
desktop publishing
development
documentation
Access Control (Users/Casts)
Specify the User(s) and/or Cast(s) that may control this list.
Users
Casts
aabbott
aandrews
adam
Administrator
anelson
athomas
bartis
bdavis
Show all
Show none
Search
Search
Access Control (Permissions)
Specify the initial permissions for the User(s) and/or Cast(s) selected above.
Delete Modify Report Schedule
Add>

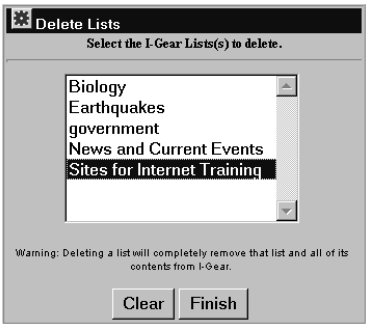
Click the **Add** button. The next display will allow you to populate the new List with URLs.

You may add as many URLs as necessary to the new List. (For more detailed information on adding URLs to local Lists, see “Adding URLs to Lists” on page 108.)

Note: When a List is initially created, the default state is Off. If you want the default setting for a public List to be some setting other than Off, you must go to the Schedule method for the System object and change the default state for the List. The state of a List still can be scheduled differently for each object; setting the default state only specifies its initial default behavior. For example, a List that contains the host names of your administrative Intranet servers can be set to Deny for a student Cast but Allow (Filtering Disabled) for a teacher Cast; the default state for this List could remain Off. For more information on Lists and List states, see "Understanding Filter Lists and DDR" on page 9.

Deleting a List

To delete a List, click the Delete link from the List administration page or the List Delete shortcut from the main I-Gear administration page.



Select one or more List objects to delete. Then click the **Finish** button.

Note: Only locally created Lists (i.e., not the predefined Content Category Lists provided by URLabs) may be deleted.

Warning: When a List is deleted, all URLs that populate that List are lost.

Modifying a List

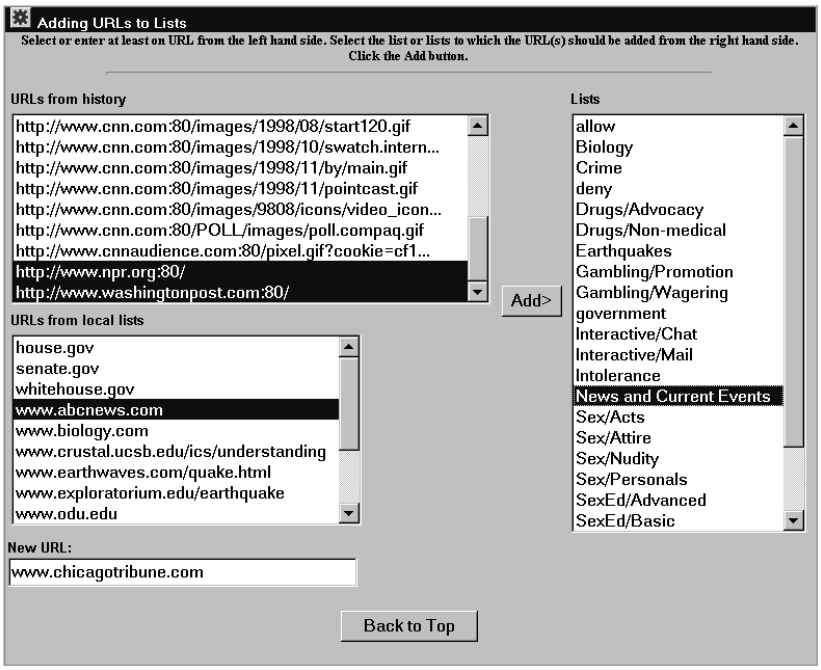
The Modify method for the List object allows you to add and delete URLs from local Lists, as well as change the Access Control List features.

To modify a List, click the Modify link from the List object administration page or the List Modify shortcut from the main I-Gear administration page.

Adding URLs to Lists

I-Gear looks for the most exact match when checking a URL against assigned Lists. Thus, by customizing your local Lists, you can block or allow individual Web pages or entire directories, machines, or domains. For additional guidance on adding URLs to local Lists, see “Adding URLs to Lists” on page 15.

To add URLs to a List, select Add URLs to Lists from the menu on the right, and click the **Next** button. (You specify the List(s) to which you wish to add URLs from the next display.)



You may add as many URLs as necessary to selected List(s). The left side of the display shows your recent history (i.e., the most recent 20 sites visited) so that you can conveniently select any site(s) you have recently accessed to add to a List. Also listed on the left are URLs that already are contained in any locally created List(s) so that you can conveniently recategorize any previously identified URLs. Select as many URL(s) as necessary from either or both of these lists on the left. A field is also provided so that you can manually enter any additional URLs you wish to add. After you have selected the appropriate URLs and/or entered a new URL, select the appropriate List(s) from the right side of

the display, and click the **Add** button. I-Gear will provide confirmation that your changes have been made.

Note: Remember that for each request for Internet access, I-Gear checks the local versions of all active Content Category Lists before it checks the URLabs versions. If I-Gear finds a match in one or more active local Lists (i.e., Lists that are not in the Off state), it will not check the URLabs versions of the Lists. Thus, you can completely override any URLabs categorization of a site by adding a site to a local List, and you can add additional sites not contained in the URLabs-provided Lists.

Note: Keep in mind when you are adding URLs to your local Lists that Deny Lists override Allow Lists. Thus, if you place a URL in more than one List and one of these Lists is in the Deny state and the other is in an Allow state, access to the URL will be denied.

Note: With I-Gear for FireWall-1, when you enter a URL in a local List, I-Gear attempts to identify all IP addresses associated with that URL. (I-Gear for FireWall-1 has access to only actual IP addresses rather than the domain names.) Note that the List of IP addresses obtained by I-Gear may not be complete and is subject to periodic change. Periodic review and update of the IP addresses contained in local Lists are necessary in maintaining the accuracy of your local Lists.

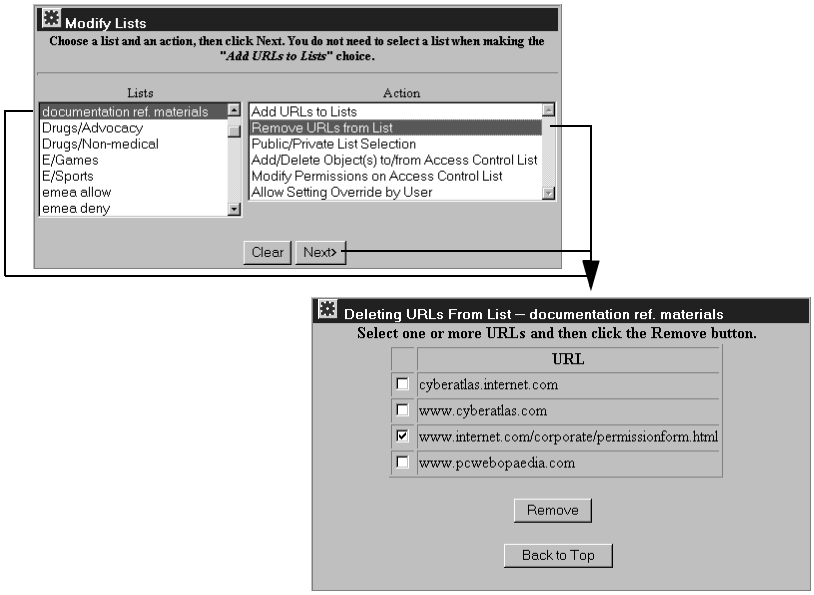
When you have finished adding URLs to Lists, click the **Back to Top** button to return to the main I-Gear administration page.

Removing URLs from Lists

To delete URLs from a List, select the appropriate List, select Remove URLs from Lists from the menu on the right, and click the **Next** button.

The URLs currently in the selected List are displayed. Select the URL(s) to be removed from the List by clicking the check box(es) next to the URL(s). When you have checked the URLs you wish to remove from the List, click the **Remove** button.

Note: Only URLs from the local versions of the Content Category Lists can be deleted. The URLs added by URLabs to the predefined Lists cannot be deleted (and are not shown in the display).



I-Gear will provide confirmation that your changes have been made. Click the **Done** button to return to the main I-Gear administration page.

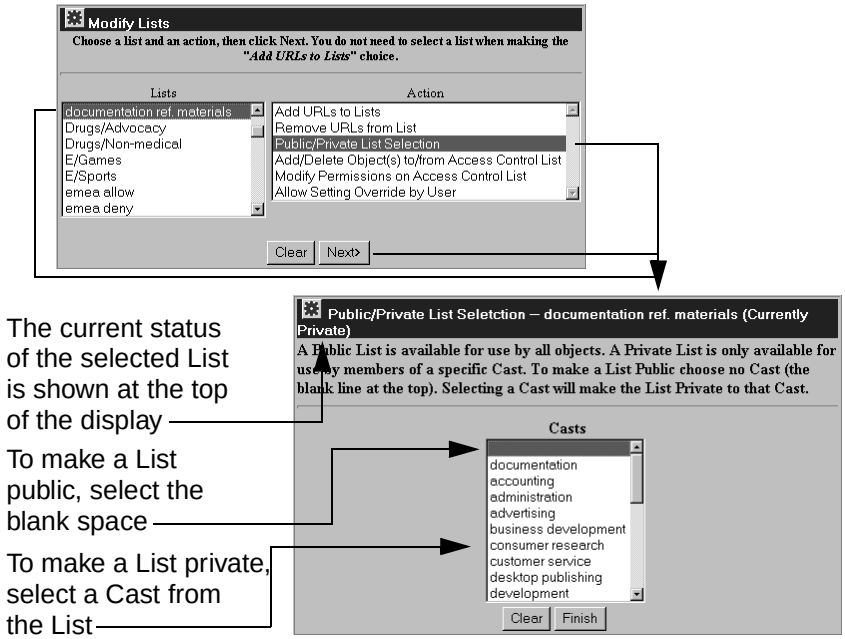
Changing the Public/Private Status for a List

To change the status of a List, select Public/Private List Selection from the menu, and click the **Next** button.

Note: A public List is available to all objects. A private List is only available for use by a specific Cast.

The top of the next display indicates the current status of the selected List. To make a private List public, select the blank space (no Cast) at the top of the list of Casts. To make a public List private, select the

appropriate Cast from the list. Click the **Finish** button. I-Gear will confirm that your changes have been made successfully.


Modify Lists
Choose a list and an action, then click Next. You do not need to select a list when making the "Add URLs to Lists" choice.
Lists
Action
documentation ref. materials
Drugs/Advocacy
Drugs/Non-medical
E/Games
E/Sports
emea allow
emea deny
Add URLs to Lists
Remove URLs from List
Public/Private List Selection
Add/Delete Object(s) to/from Access Control List
Modify Permissions on Access Control List
Allow Setting Override by User
Clear
Next>
Public/Private List Seletction – documentation ref. materials (Currently Private)
A Public List is available for use by all objects. A Private List is only available for use by members of a specific Cast. To make a List Public choose no Cast (the blank line at the top). Selecting a Cast will make the List Private to that Cast.
Casts
documentation
accounting
administration
advertising
business development
consumer research
customer service
desktop publishing
development
Clear
Finish
The current status of the selected List is shown at the top of the display
To make a List public, select the blank space
To make a List private, select a Cast from the List

Adding/Deleting Object(s) to/from Access Control List

Adding objects to and deleting objects from Access Control Lists is the same for the Client, User, Cast, and List objects. Refer to “Adding/Deleting Objects to/from the Access Control List (Enterprise version only)” on page 53 for detailed procedures on adding objects to and deleting objects from Access Control Lists.

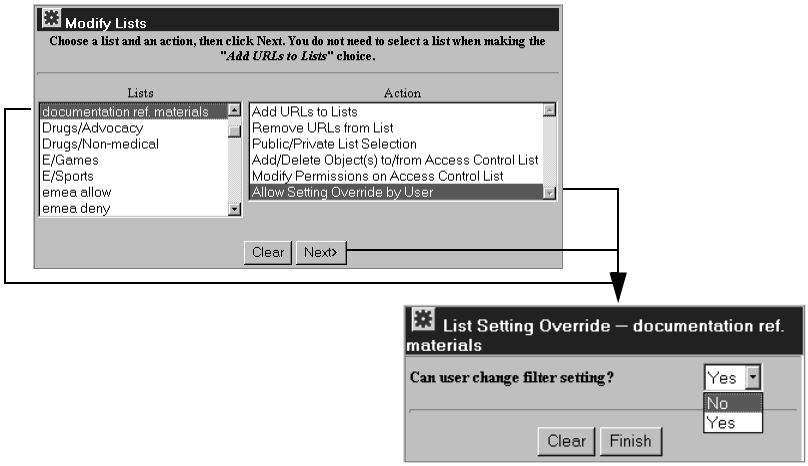
Modifying Permissions on Access Control List

Modifying the permissions for objects on Access Control Lists is the same for the Client, User, Cast, and List objects. Refer to “Modifying Permissions on Access Control List (Enterprise version only)” on page 55 for detailed procedures on modifying the permissions for objects on Access Control Lists.

Changing the Filtering Override Setting for a List

To change the filtering override setting for a List, select the appropriate list, select Allow Setting Override by User from the menu on the right side of the display, and click the **Next** button.

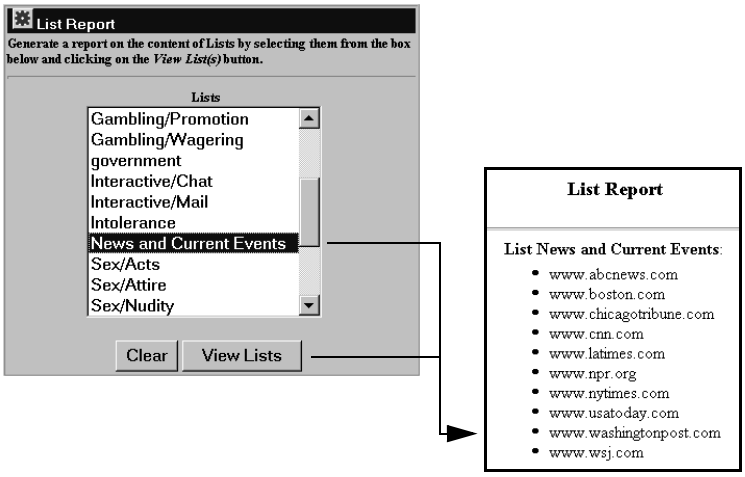
From the next display, indicate whether the filtering state of the List can be overridden by Users (by scheduling an event for a User or Cast). This restriction does not apply to Users who have Schedule permission for the System object. Then click the **Finish** button. I-Gear will confirm that your changes have been made successfully.



Generating a Report for a List

The Report method for the List object enables you to review the locally added URLs for a given List. To generate a report for a given List, click the Report link from the List administration page or the List Report shortcut from the main I-Gear administration page.

Select the desired List(s) and click the **View Lists** button. I-Gear will display all locally added URLs for the selected List.



10. Working with the Dictionary Object

Modifying a Dictionary

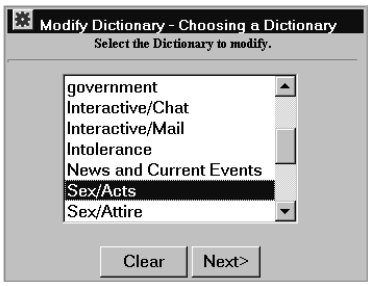
The Modify method for the Dictionary object allows you to add or delete words from the local versions of Dictionaries.

Each of I-Gear's predefined Lists has an associated Dictionary populated with trigger words by URLabs. A local version of each Dictionary is also provided so that you can add words as necessary, based on your specific requirements. In addition, when you create a new List in I-Gear, a corresponding Dictionary of the same title is automatically created so you can add any words to be scored for that Lists, if necessary. When you add words to a local Dictionary, you must provide a point value for each word or phrase for use in DDR scoring.

Note: Words manually added into the local version of a Dictionary (for the predefined Content Category Lists provided by URLabs) override any URLabs-provided Dictionary entries for the same word.

Note: Each Dictionary in I-Gear is associated with a corresponding List; thus, the words in the Dictionary are used by DDR only when the corresponding List is in effect. For example, if the word *snorteskle* were added in the Sex/Acts List, the word would be scored by DDR only if the filter List Sex/Acts were active and in the Deny or Allow (Filtering Enabled) state.

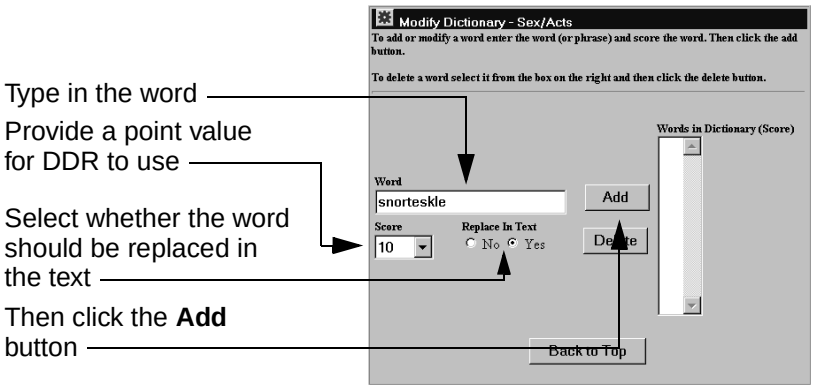
To add or delete a word or phrase in a Dictionary, click the Modify link from the Dictionary administration page or the Dictionary Modify shortcut from the main I-Gear administration page.



Select the Dictionary object to be modified. Then click the **Next** button.

Adding Words to Dictionaries

Enter the word or phrase to be added and provide a point value from the available range to be used in DDR scoring. Also select whether the word or phrase should be replaced in the text (i.e., if the particular word appears in, for example, the page description returned by a search engine, then that word would be replaced in the text displayed on the screen). Then click the **Add** button. When you have finished adding words to the Dictionary, click the **Back to Top** button.

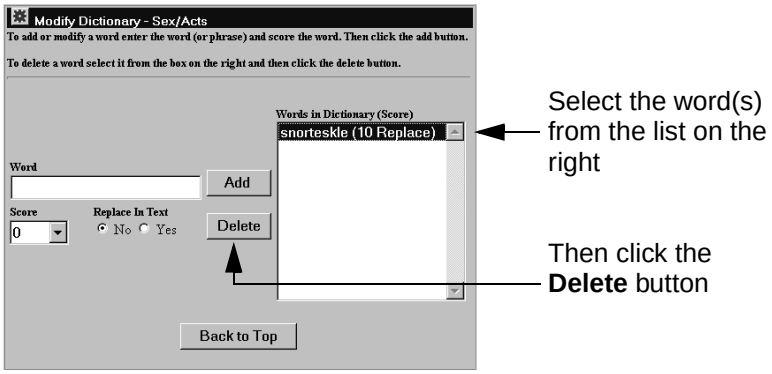

Type in the word
Provide a point value for DDR to use
Select whether the word should be replaced in the text
Then click the **Add** button
Modify Dictionary - Sex/Acts
To add or modify a word enter the word (or phrase) and score the word. Then click the add button.
To delete a word select it from the box on the right and then click the delete button.
Words in Dictionary (Score)
Word
snorteskle
Add
Score
10
Replace In Text
No
Yes
Delete
Back to Top

Note: In assigning point values to words you have added to a Dictionary, you can use negative scores for words to offset blocking. For example, if you found that DDR was blocking a number of URLs that contained useful clinical discussions of circumcision, you could try adding the word "surgeon" (or another word that appears on the pages in question) to the Sex Ed/Basic Dictionary with a negative score to potentially offset the blocking of these particular sites. Once you alter a Dictionary, you should experiment with attempting to access sites to determine whether DDR is performing appropriately.

Warning: Do not be overly aggressive in adding "conditionally" objectionable words to the Dictionary. Entering words such as "sex" or "bottom" will likely cause many more pages to be blocked than you probably intend.

Deleting Words from Dictionaries

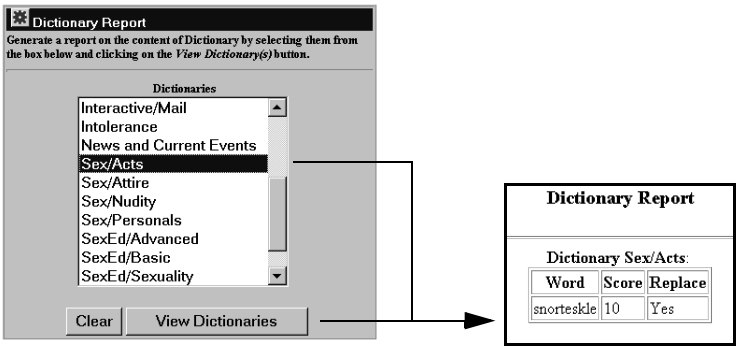
Select one or more words from the list on the right side of the display. Then click the **Delete** button. When you have finished deleting words from the Dictionary, click the **Back to Top** button.


Modify Dictionary - Sex/Acts
To add or modify a word enter the word (or phrase) and score the word. Then click the add button.
To delete a word select it from the box on the right and then click the delete button.
Words in Dictionary (Score)
snorteskle (10 Replace)
Word
Add
Score
Replace In Text
No Yes
0
Delete
Back to Top
Select the word(s) from the list on the right
Then click the **Delete** button

Generating a Report for a Dictionary

The Dictionary Report allows you to review locally added words and phrases in selected Dictionaries and associated scoring properties. To access the Dictionary Report method, click the Report link from the Dictionary administration page or the Dictionary Report shortcut from the main I-Gear administration page.

Then select the desired category and click the **View Dictionaries** button.



The locally added words and the associated scoring properties will be displayed for the selected Dictionary.

11. Working with the System Object

Modifying the System

The Modify method for the System object allows you to modify the proxy, cache, and RADIUS configurations; the built-in HTTP server options; I-Gear licensing; and other System attributes. If you subscribe to List updates, you can also manually initiate a download of the updated predefined Content Category Lists and Dictionaries. You can also back up the I-Gear configuration, as well as restore these backed up files using the Modify method for the System object.

To modify the System object, click the Modify link from the System object administration page or the System Modify shortcut from the main I-Gear administration page.

Modifying the Proxy Configuration

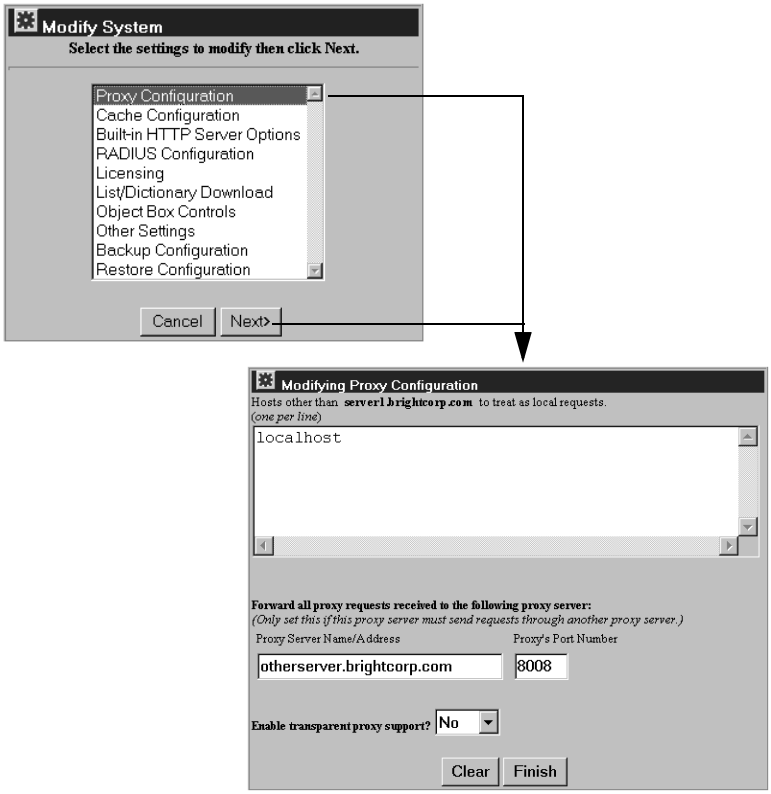
To modify the proxy configuration, select Proxy Configuration from the menu provided, and click the **Next** button. From the next display, enter the appropriate information as discussed below.

If the server running I-Gear has more than one name by which it can be identified, you must specify the other host names so that I-Gear treats any requests using these alternate host names as local requests. Enter the name(s) (one per line) of any other host names by which the server running I-Gear can be identified, if applicable.

In a standard configuration, the server running I-Gear functions as the proxy server for all Internet requests. However, if your particular network configuration requires the I-Gear server to proxy all Internet requests through another server (called “proxy chaining”), you must specify those proxy settings. If you have established proxy chaining, enter the name or the IP address of the server through which you want I-Gear to proxy Internet requests and the appropriate port number.

I-Gear can be set to handle a transparent proxy setup. If your network has been set to transparently proxy all HTTP requests through the server running I-Gear, you must enable transparent proxy support for I-Gear. Set the transparent proxy support setting to Yes, if applicable. When you have finished entering the necessary information, click the **Finish** button.

Note: Changing your proxy settings here has no effect on the browser settings on Client workstations. The browser settings should remain set to proxy through the server running I-Gear.



Modifying the Cache Configuration

The Cache Configuration settings allow you to change the amount of system memory dedicated to caching, the disk space allocated to caching, and the grace periods that specify when information expires from the cache. You can also specify any sites that you do not want cached by I-Gear. To modify the cache configuration, select Cache Configuration from the menu, and click the **Next** button.

Note: If you are using FireWall-1 and are using I-Gear transparently as a Content Vectoring Protocol (CVP) resource or if you are using I-Gear purely as a plug-in for Microsoft Proxy Server, then the caching feature of I-Gear will not function and these settings do not apply. However, if you are running I-Gear concurrently with FireWall-1 or Microsoft Proxy Server and you have configured any browser Clients to use the I-Gear

proxy server, then the caching feature is operational and these settings do apply.

Select the maximum system memory to be used by the cache. This setting allocates the maximum amount of system memory dedicated to tracking the sites that have been cached.

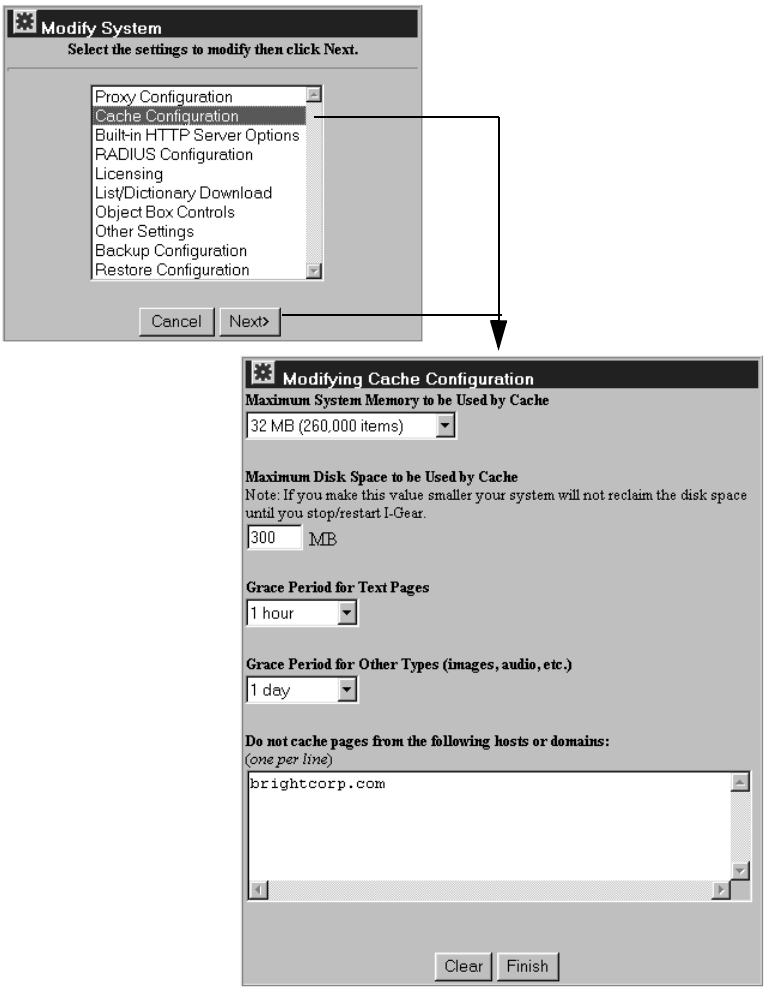
Select the maximum disk space to be used by the cache. The number you entered at installation should appear as the default in this field. A minimum of 100 MB is recommended for this setting.

Note: If you are using I-Gear with Windows NT and you reduce the amount of disk space dedicated to caching, you must wait several minutes and then shut down I-Gear and restart to properly free up the specified amount of disk space.

Select the desired grace periods for specifying when information expires from the cache. Two separate settings are provided: one for text pages and one for other types of information (e.g., images, audio). (The grace period is the amount of time during which a site can be retrieved from the cache without some data being exchanged with the actual site to verify whether the site has been changed.) Many sites provide information on the next time the site will be updated. In these cases, I-Gear honors the grace period specified by the site. However, if no grace period is specified, these settings apply as appropriate. The default settings are 1 hour for text pages and 1 day (24 hours) for other types of information.

Enter any hosts or domains that you do not want cached in the field provided (one entry per line). Normally, a Web site provides information on whether or not a site is cacheable, and I-Gear follows the caching directives specified by the site. However, in some cases certain sites have been incorrectly coded, and I-Gear will incorrectly cache pages that generally should not be cached. To correct for this problem, the host names or domains can be entered in this field to prevent I-Gear from caching pages from these sites.

When you have made the necessary changes, click the **Finish** button.



Note: To change the storage location of the cache on your system, contact URLabs Support Services.

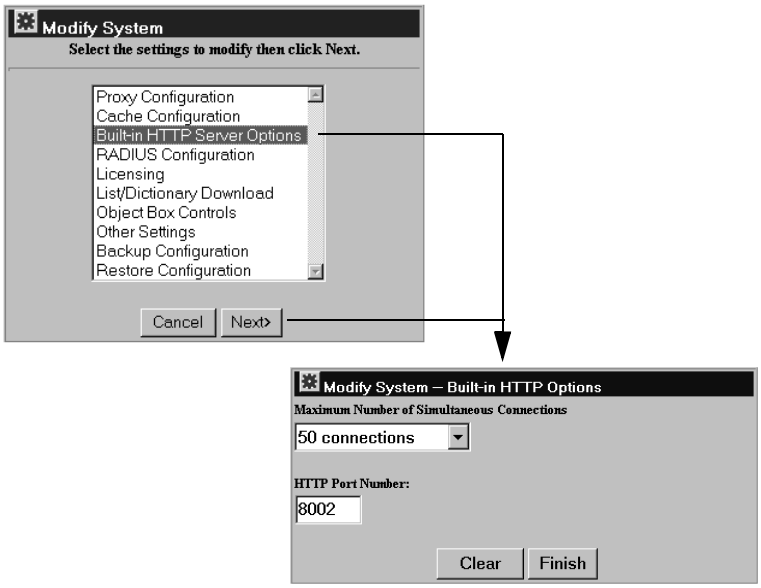
Modifying the Built-in HTTP Server Options

To modify the built-in HTTP server options, select Built-in HTTP Server Options from the menu, and click the **Next** button.

Select the appropriate number of simultaneous connections to I-Gear from the range shown in the pull-down menu. The number of connections that you enable should be some fraction of the total number of Cli-

ent machines you have on your network (the total number of Client machines being the maximum number of simultaneous connections that would be possible on your network) and should be based to some degree on the available memory (because each simultaneous request will use additional memory).

If you need to change the port number, enter the new number in the space provided (port number 8002 is the default port number for I-Gear). You should only need to change the port number to avoid conflict with another application, which should occur only in rare instances. After you have made the necessary changes, click the **Finish** button.



Note: If during periods of high network usage the number of requests to I-Gear exceeds the specified number of simultaneous connections, then each additional request is queued and processed as soon as another request is completed.

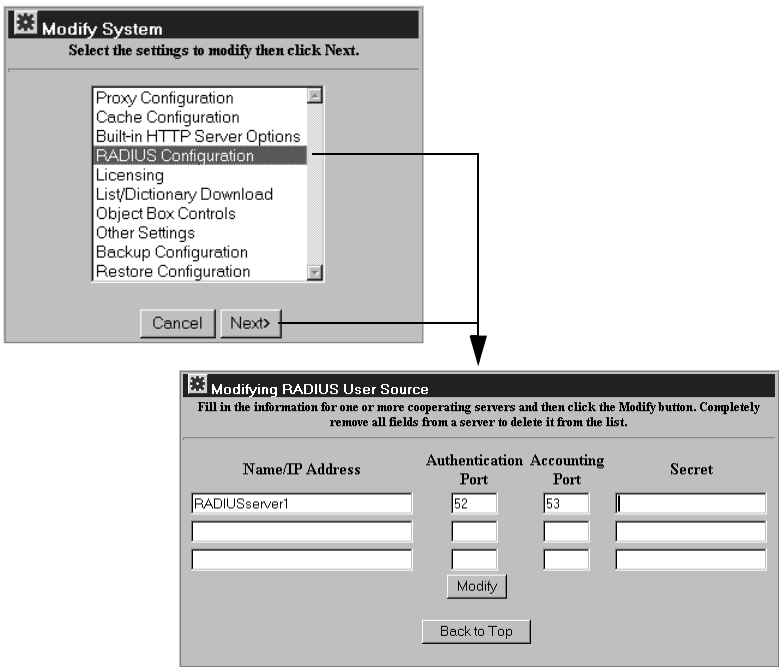
Note: In setting the number of simultaneous connections, take into account the following considerations. Generally, the higher the number of connections allowed, the more overhead that is required to support these connections, which may slow performance. Thus, you need to consider network performance and available memory when selecting the number of simultaneous connections. On the other hand, if the number of simultaneous connections is set too low, too few resources will be available to handle network delays that may be encountered. Most sites

will not require this number to be higher than 50 (50 is the default value and the recommended setting).

Modifying the RADIUS Configuration (Enterprise version only)

If you have purchased the Enterprise version of I-Gear and you are using RADIUS server(s), you must configure I-Gear to interface with the appropriate RADIUS server(s) on your network. To modify the RADIUS configuration, select RADIUS Configuration from the menu, and click the **Next** button.

From the next display, enter the IP address or host name for those RADIUS servers with which I-Gear will need to share information. Also enter the authentication and accounting port numbers, as well as the secret (encryption) information needed. Click the **Modify** button to save your changes. I-Gear will provide confirmation that your changes have been made successfully.



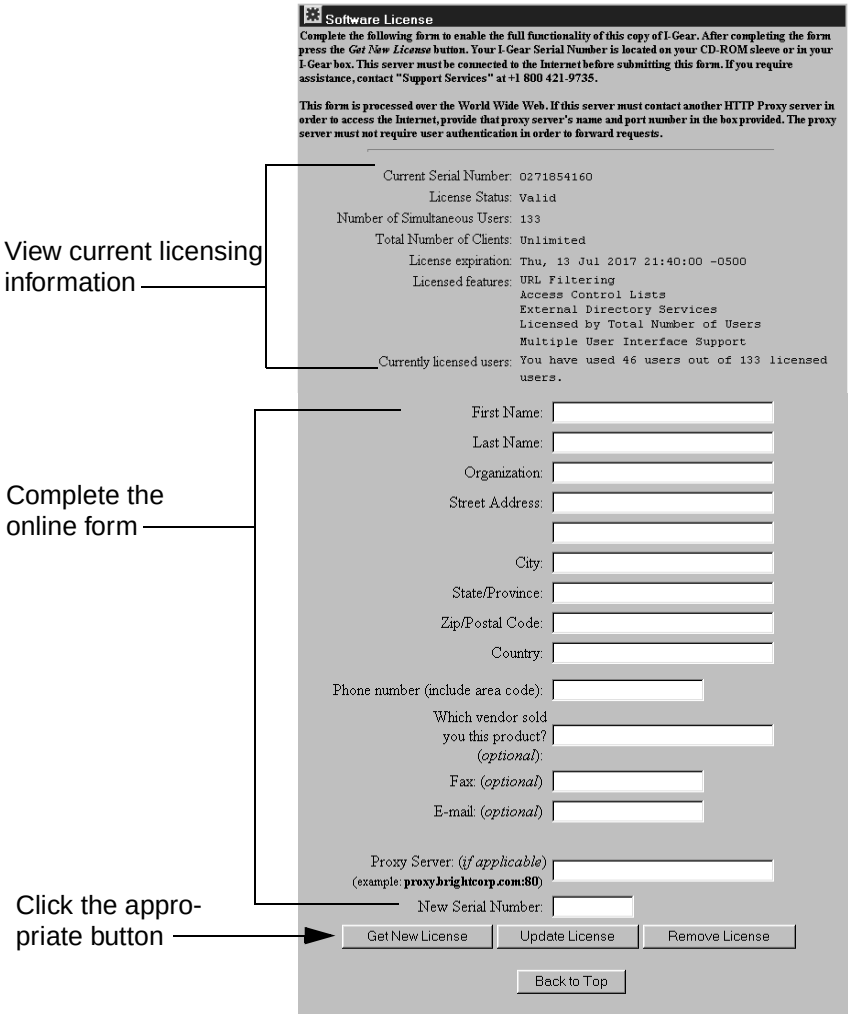
Note: You must add all RADIUS Users who will be utilizing the I-Gear software to I-Gear using the Add method for the User object.

Note: You must define one or more RADIUS servers here before RADIUS Users can authenticate through I-Gear.

Modifying I-Gear Licensing

To modify your I-Gear licensing, select Licensing from the menu provided. Then click the **Next** button.

The next display shows the currently installed serial number and license status, the number of simultaneous Users, the total number of Clients permitted, and the licensed features (Enterprise version only) based on your current licensing agreement. The expiration date for the current license is also shown. If you have just installed I-Gear, this information will not be filled in, and the license status should read “invalid.”


Software License
Complete the following form to enable the full functionality of this copy of I-Gear. After completing the form press the Get New License button. Your I-Gear Serial Number is located on your CD-ROM sleeve or in your I-Gear box. This server must be connected to the Internet before submitting this form. If you require assistance, contact "Support Services" at +1 800 421-9735.
This form is processed over the World Wide Web. If this server must contact another HTTP Proxy server in order to access the Internet, provide that proxy server's name and port number in the box provided. The proxy server must not require user authentication in order to forward requests.
Current Serial Number: 0271854160
License Status: Valid
Number of Simultaneous Users: 133
Total Number of Clients: Unlimited
License expiration: Thu, 13 Jul 2017 21:40:00 -0500
Licensed features: URL Filtering
Access Control Lists
External Directory Services
Licensed by Total Number of Users
Multiple User Interface Support
Currently licensed users: You have used 46 users out of 133 licensed users.
First Name:
Last Name:
Organization:
Street Address:
City:
State/Province:
Zip/Postal Code:
Country:
Phone number (include area code):
Which vendor sold you this product? (optional):
Fax: (optional)
E-mail: (optional)
Proxy Server: (if applicable)
(example: proxy.brightcorp.com:80)
New Serial Number:
Get New License
Update License
Remove License
Back to Top
View current licensing information
Complete the online form
Click the appropriate button

Complete the online form. If the form does not specify that the information in a particular field is optional, you must fill in that field. Your I-Gear serial number is located on the CD-ROM sleeve or in the I-Gear product box. If you are updating your license and your serial number has not changed, enter the current serial number in the appropriate field.

Note: If you do not provide the requested information, you will get back an error message stating that the requested information was not provided, and you will need to submit the form again.

Note: The I-Gear server must be connected to the Internet before you submit this form because the form is processed over the Web. If the I-Gear server must contact another HTTP proxy server in order to access the Internet, you must provide the name of that proxy server and the appropriate port number in the space provided (e.g., `proxy.brightcorp.com:80`).

Once you have filled in the form, click the appropriate button to modify your I-Gear license, as described in the table below.

Button	Description
Get New License	Use this button to install an entirely new license. This button is often used by sites that have an evaluation (temporary) I-Gear license and then decide to purchase the product. Use this button to input the new (permanent) serial number that is included with the purchased copy of I-Gear.
Update License	Use this button to retrieve updated license parameters (such as the maximum number of simultaneous users or the license expiration date). This button is often used by sites that have purchased add-ons such as additional user licenses. After activating the certificate included with such an add-on kit (by following the instructions included with each kit), this button should be used to propagate the new license information into I-Gear.
Remove License	Use this button to delete your license. If you delete your license, I-Gear will operate as a proxy in guest mode—all other functionality will be lost.

Note: I-Gear will confirm that your new license information has been processed, and the licensing information should update. If a problem is encountered, you will get back a list of error messages. Retain these messages so that you can relate them to URLabs Support Services if necessary.

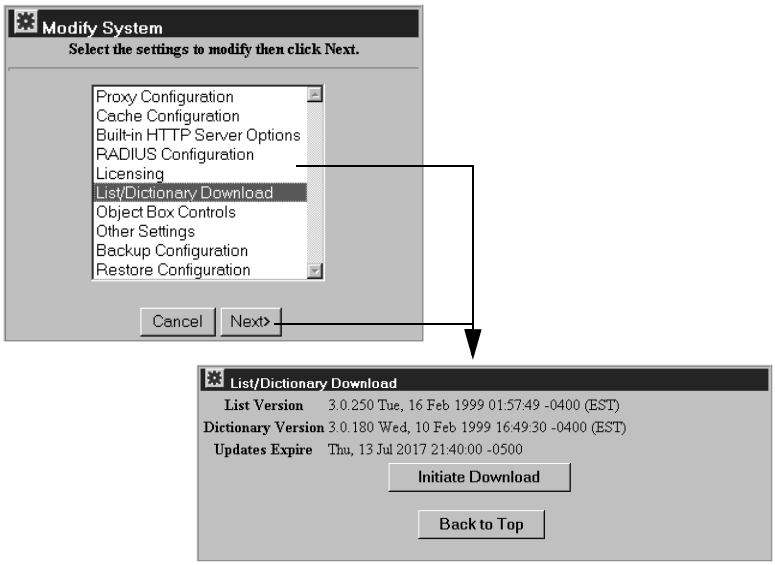
If you have problems updating your licensing, call URLabs Support Services at +1 800 421-9735.

Initiating List/Dictionary Download

I-Gear's predefined Content Category Lists and Dictionaries are continually updated by URLabs. I-Gear automatically polls URLabs several times a day to determine whether updated versions have been posted. If new versions have been posted, I-Gear automatically initiates a download. However, you can manually initiate a download at a particular time, if necessary. You can also check to see which versions of the Lists and Dictionaries I-Gear is currently using and the date and time these versions were created. You can also check this display to see when your current subscription to the List updates expires.

Note: If you do not subscribe to List updates, you will not be able to download updated Lists, and the URLabs Lists you are currently using will be deleted.

To check the version of Content Category Lists or Dictionaries I-Gear is currently using, to determine when your List update subscription expires, or to initiate a List/Dictionary download, select List/Dictionary Download from the menu. Then click the **Next** button.



The next display shows the version numbers for the Lists and Dictionaries currently being used by I-Gear and the date and time these versions

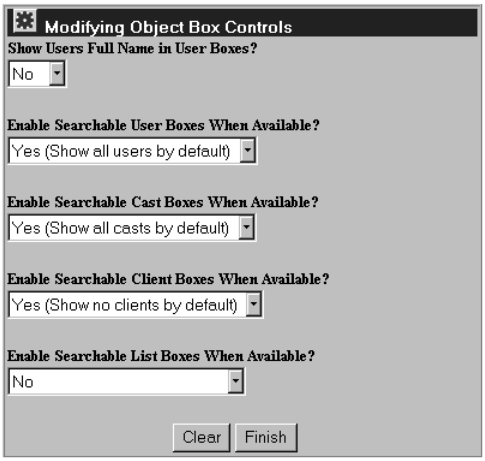
were created. The display also shows the date your update subscription expires. If you are using a limited-time license (e.g., a demo copy of the software), the date the updates expire should also be the date your license expires.

If you want to manually initiate a download, click the **Initiate Download** button. I-Gear will confirm that a download has been initiated. Click the **Done** button to return to the I-Gear administrative interface. I-Gear will first check to see if a new version is available; if so, the download will occur in the background. You should recheck the version numbers in a few minutes to see whether an updated list has been posted.

Note: Filtering will NOT be affected during a List/Dictionary download.

Modifying Object Box Controls

To modify the object box controls (i.e., activate the search capability for selected objects), select Object Box Controls from the menu, and click the **Next** button.


Modifying Object Box Controls
Show Users Full Name in User Boxes?
No
Enable Searchable User Boxes When Available?
Yes (Show all users by default)
Enable Searchable Cast Boxes When Available?
Yes (Show all casts by default)
Enable Searchable Client Boxes When Available?
Yes (Show no clients by default)
Enable Searchable List Boxes When Available?
No
Clear
Finish

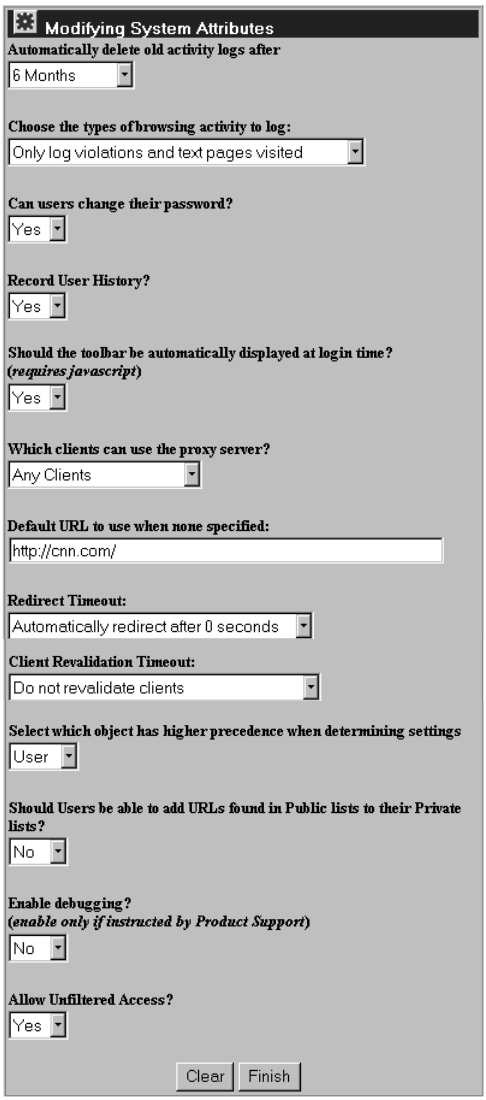
From the next display, activate the search capability for the desired objects. For information on using the search capability, see “Search Capability for Object Lists” on page 44.

Setting	Description
Show user’s full name in User box?	Select whether to display the User’s full name in brackets next to the account name, for those I-Gear functions that include lists of User accounts, such as the Delete User function. **Note:** If this feature is turned off, then lists of accounts would include only the actual account name, for example, `ayates`. If this feature is turned on, then the same display would show the following entry for the same account: `ayates [Andrew Yates]`. **Note:** For sites with large numbers of System Users, selecting Yes to display users’ full names may cause I-Gear to take more time in loading lists of user accounts because I-Gear must request this information from the system.
Enable searchable User boxes when available?	Select whether to enable the search capability for functions that include lists of Users (e.g., the Delete a User display). If you do not want the search capability activated, select “no.” To enable the search capability, select either Yes (Show all Users by Default) or Yes (Show no Users by Default). **Note:** For sites with large numbers of users, selecting the Yes (Show All Users by Default) option to activate the search capability may cause I-Gear to take more time in loading lists of user accounts.
Enable searchable Cast boxes when available?	Select whether to enable the search capability for functions that include lists of Casts (e.g., the Delete a Cast display). If you do not want the search capability activated, select “no.” To enable the search capability, select either Yes (Show all Casts by Default) or Yes (Show no Casts by Default).
Enable searchable Client boxes when available?	Select whether to enable the search capability for functions that include lists of Clients (e.g., the Delete a Client display). If you do not want the search capability activated, select “no.” To enable the search capability, select either Yes (Show all Clients by Default) or Yes (Show no Clients by Default).
Enable searchable List boxes when available?	Select whether to enable the search capability for functions that include lists of Lists (e.g., the Modify a List display). If you do not want the search capability activated, select “no.” To enable the search capability, select either Yes (Show all Lists by Default) or Yes (Show no Lists by Default).

After you have made the necessary changes, click the **Finish** button.

Modifying Other Settings

To modify other system attributes, select Other Settings from the menu, and click the **Next** button.



The system attributes that can be modified from this display are described in the following table.

Setting	Description
Delete activity logs	Select the length of time that I-Gear should retain activity logs.
Type of browsing activity to log	Select the type of browsing activity that I-Gear should log. You can specify no activity, violations only, violations and text pages visited, or all activity (including text, images, audio, etc.). **Warning:** Many of the report functions will not operate if activity logging is disabled. **Note:** This setting applies to browsing activity only. Administrative functions are always logged, and logging of administrative activity cannot be disabled. **Note:** Remember that the settings for specific Clients, Users, and Casts may be inherited from the System default settings for logging browsing activity.
Can users change their passwords?	Select the System default setting for whether Users can change their passwords. **Note:** Remember that the settings for specific Users and Casts may be inherited from the System default settings for changing passwords.
Record user history?	Specify whether I-Gear should retain User history. **Note:** If history logging is disabled, Users will not be able to view their browsing history when they click the **History** button on the I-Gear tool bar.
Display tool bar automatically at login?	Specify whether I-Gear should automatically display the tool bar at login. If you select "No," Users will need to visit the URL `http://<servername>:port/toolbar` to invoke the tool bar. **Note:** Remember that JavaScript must be enabled to automatically display the tool bar.

Setting	Description
Which clients can use the proxy server?	Specify which Clients can use the proxy server: any client or authorized Clients only. **Note:** If your license is limited to a specific number of authorized Clients, this setting is not applicable (you do not need to worry about which setting is displayed here) because you are already limited to authorized Clients only. If your license allows an unlimited number of Clients, you can select Authorized Clients Only here to limit the Clients that can use the proxy server to only those you have authorized (using the Add method for the Client object). (You can remove the authorized status of clients using the Delete method for the Client object.) See "Working with the Client Object" on page 49 for more details on authorized versus unauthorized Clients.
Default URL to use when none specified	Specify the default URL to display when no other URL has been requested (i.e., the URL that the browser will display automatically after a User has clicked the **Login** button).
Redirect timeout	Select the length of time the I-Gear Login Completed page will remain on the screen after a successful login. To make the Login Completed page appear only briefly, select "0 seconds."
Client revalidation timeout	Select the desired period of inactivity after which I-Gear will challenge the Client browser for a cookie to ensure that the User has not changed. **Note:** This setting can be used in situations in which pools of IP addresses are distributed randomly to Users as needed, to prevent a second User (having received the same IP address as the first User) from browsing under the first User's permissions if the first User did not log out of I-Gear. **Note:** This option is not available if you are using I-Gear for FireWall-1.
Select which object has higher precedence when determining settings	Select the object (i.e., Client or User) that has the highest priority in terms of object permissions. For more information, see the section entitled "Hierarchy of Permissions" on page 6.
Should Users be able to add URLs found in Public lists to their Private lists?	Specify whether Users with access control for Private Lists (through the Family interface) can add URLs that are found in any Public list to a Private list. **Note:** This setting prevents Users from adding any URLs that are found in Public lists to their Private list(s) to override filtering settings that may have been established for the Public list.

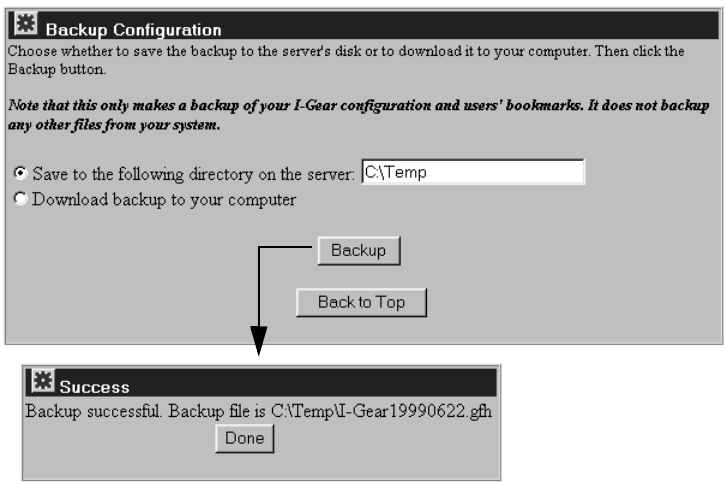
Setting	Description
Enable debugging?	Enable or disable the debugging feature. When the debugging feature is enabled, URLabs Product Support can connect to the system to obtain access to error messaging to resolve a problem. **Note:** During normal operation of I-Gear, the debugging feature should be disabled. This setting should ONLY be enabled when requested by URLabs Product Support personnel and should be disabled immediately after the problem has been resolved.
Can grant unfiltered access?	Specify whether a User can grant Unfiltered (or Audit Mode) access to another User using the Family administrative interface. **Note:** If this setting is set to No, the Unfiltered and Audit Mode filtering settings are not available in the Family interface. In addition, the 2-minute administrative override for blocked sites (normally available to Users with administrative permissions) is not available.

When you have finished making the desired changes, click the **Finish** button.

Backing Up the I-Gear Configuration

To back up the I-Gear configuration, select Back Up Configuration from the menu, and click the **Next** button.

From the next display, choose whether to save the backup file to the server that is running I-Gear (you must specify a directory) or to download it to your local computer.


Backup Configuration
Choose whether to save the backup to the server's disk or to download it to your computer. Then click the Backup button.
Note that this only makes a backup of your I-Gear configuration and users' bookmarks. It does not backup any other files from your system.
Save to the following directory on the server: C:\Temp
Download backup to your computer
Backup
Back to Top
Success
Backup successful. Backup file is C:\Temp\I-Gear19990622.gfh
Done

Note: This feature allows you to back up the I-Gear configuration (e.g., Cast attributes and Cast memberships, user bookmarks, scheduled events, and so on). No other system files are included in this backup. You can save the backup files to a directory on the server that is running I-Gear, or you can elect to save the files directly to your local computer.

If you have elected to save the backup file to the server running I-Gear, the backup file will be named automatically. (This file will end in .gfh.) Remember the file name that is shown on the confirmation screen.

If you have elected to download the backup file to your local computer, you will be prompted to specify a location on your computer. The backup file will be given a default name by the browser. You can change this file name if necessary.

After you have made the appropriate selection, click the **Backup** button.

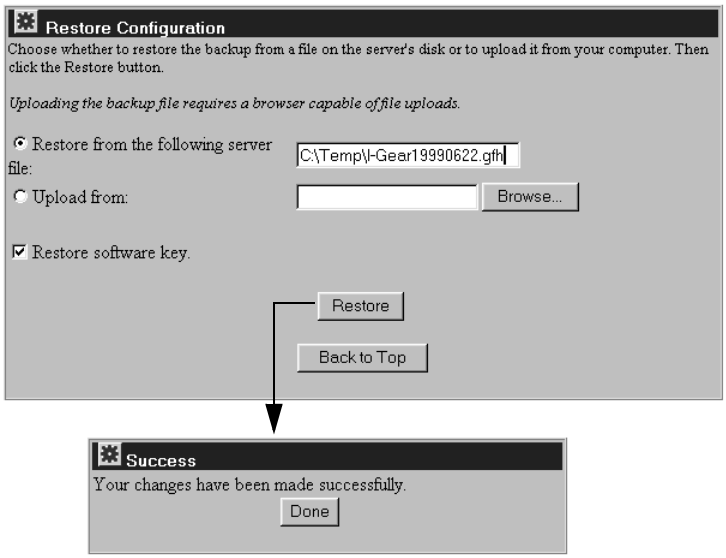
I-Gear will provide confirmation that the backup has been accomplished. Click the **Done** button to return to the I-Gear administrative interface.

Restoring a Backed-up Configuration

To restore an I-Gear configuration from backup, select Restore Configuration from the menu, and click the **Next** button.

From the next display, choose whether to restore the backup from a file already on the server or to upload it from your local computer. If you are restoring the backup from a file on the server, provide the path in the field provided. If you are uploading the file from another computer, provide the name of the computer and then click the **Browse** button. Then select the appropriate file from the local computer, and click the **Open** button.

Then select whether to restore the software key, and click the **Restore** button.


Restore Configuration
Choose whether to restore the backup from a file on the server's disk or to upload it from your computer. Then click the Restore button.
Uploading the backup file requires a browser capable of file uploads.
Restore from the following server file:
C:\Temp\I-Gear19990622.gfh
Upload from:
Browse...
Restore software key.
Restore
Back to Top
Success
Your changes have been made successfully.
Done

Note: Your I-Gear license key contains unique information regarding the machine on which you are running I-Gear, as well as information specific to your licensing agreement (e.g., the number of users, your level of support, and so on). For this reason, you should only restore the license key from backup if you are reinstalling I-Gear on the same machine on your network and your license status has not changed since the backup was created. If any of this information has changed, you should reclaim your license key. See the subsection entitled “Modifying I-Gear Licensing” on page 125 for information on reclaiming your license key.

I-Gear will provide confirmation that the backup has been accomplished. Click the **Done** button to return to the I-Gear administrative interface.

Scheduling the System

The Schedule method is basically the same for Client, User, Cast, and System objects.

Note: The System object MUST have default settings; other objects can be scheduled for specific or daily events and fall back to the System defaults when no other event is in effect. Thus, you cannot delete the System object’s default settings. Keep in mind when establishing or

changing the System defaults that settings for specific Clients, Users, and Casts can be inherited from the System defaults unless they have been specifically scheduled otherwise.

Note: The predefined Content Category Lists are generally not intended to be in either of the Allow states (Filtering Enabled or Filtering Disabled) for the System default settings. Based on your local acceptable-use policies, you will probably want to place some of the predefined Lists in the Deny state (access to the URLs in the List is denied and the associated DDR Dictionary is turned on) and leave some Lists in the Off state (access to the URLs in the List is permitted and the DDR Dictionary is turned off). However, placing Lists in either of the Allow states (for the System default settings) is not recommended. See "Understanding Filter Lists and DDR" on page 9 for detailed information on Content Category Lists and List states.

For detailed procedures on scheduling events for objects, refer to the discussion in "Scheduling an Event for a Client" on page 56.

Generating a Report for the System

The Report method for the System object is basically the same as for the Client, User, and Cast objects for Access and Access Summary reporting. The only difference in System reporting for these two types of reports is discussed in the note below.

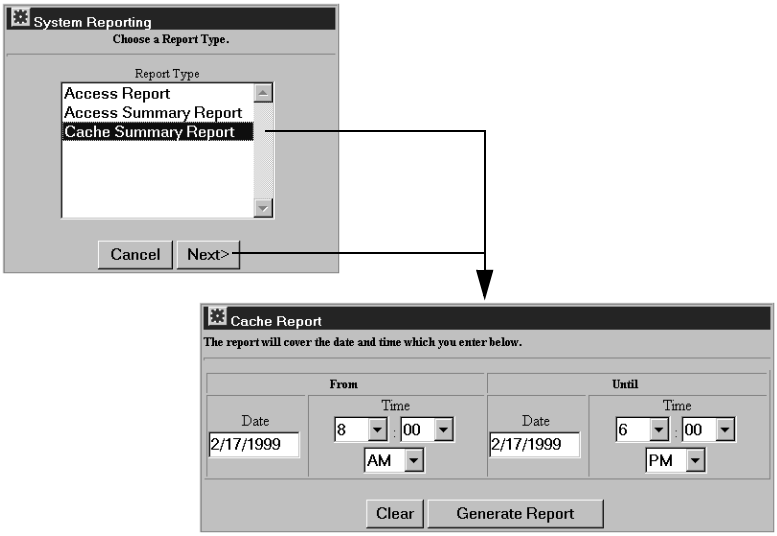
Note: For System reporting, you can report on any number of Client, User, and Cast objects simultaneously. Thus, in selecting the specific object(s) on which to report from the lists of Clients, Casts, and Users shown in the display, note that if no objects are selected the system report will include information on *all* objects.

Cache Summary Reports

A third type of Report can be generated for the System object: a Cache Summary Report. The Cache Summary Report provides summary information on, for example, the number of requests served from the cache, the size (memory and disk space) of the cache, request-processing time, and User session information.

To generate a Cache Summary Report, select the Report link from the System administration page or the System Report shortcut from the main I-Gear administration page. Then select Cache Summary Report and click the **Next** button.

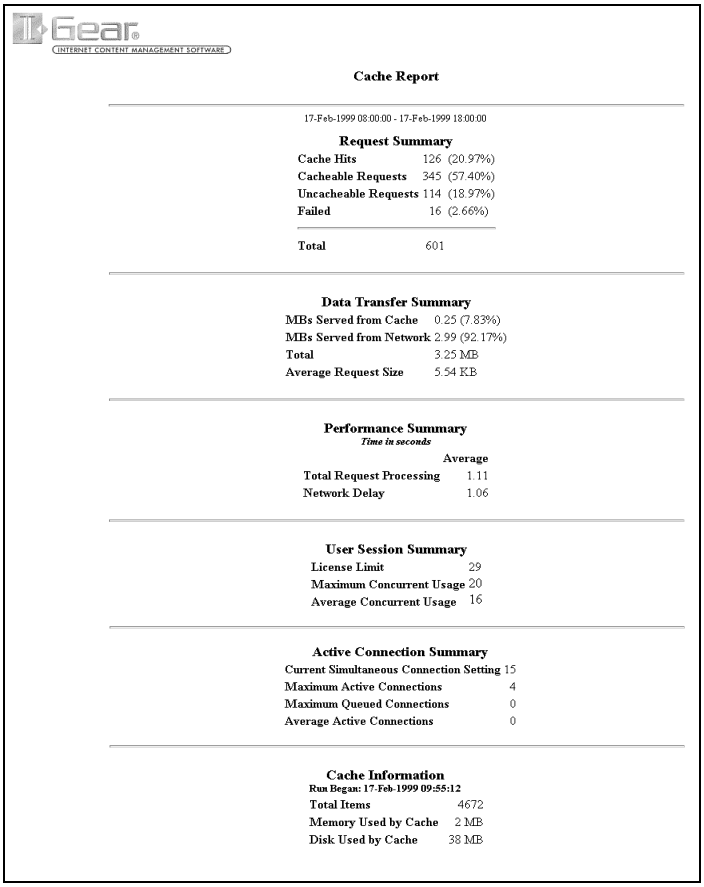
From the next display, select the date and the range of time to be covered in the report and click the **Generate Report** button.



The Cache Summary Report includes the information shown in the following table.

Report Entry	Description
Request Summary	**Cache hits.** Reports number of requests served from the cache for reported period. **Cacheable requests.** Reports number of requests not served from the cache but able to be placed in the cache for reported period. **Uncacheable requests.** Reports number of requests not served from the cache and not able to be placed in the cache for reported period. **Failed requests.** Reports number of requests that failed for reported period.
Data Transfer Summary	**MBs served from cache.** Reports number of megabytes of data served from the cache for reported period. **MBs served from network.** Reports number of megabytes of data retrieved from the network for reported period. **Total.** Reports total number of megabytes of data processed for reported period. **Average request size.** Reports average size of requests processed for reported period.

Report Entry	Description
Performance Summary	**Total request processing.** Reports average amount of time (in seconds) that I-Gear spent processing each request for reported period. **Network delay.** Reports average amount of time (in seconds) spent on network delays (e.g., waiting for a remote server to respond).
User Session Summary	**License limit.** Displays maximum number of simultaneous Users allowed by current license. **Maximum concurrent usage.** Reports maximum number of Users logged into I-Gear at any given time for reported period. **Average concurrent usage.** Reports average number of Users logged into I-Gear for reported period.
Active Connection Summary	**Current simultaneous connection setting.** Reports the current setting for the number of simultaneous connections to I-Gear. **Maximum active connections.** Reports maximum number of active connections to I-Gear at any given time for reported period. **Maximum queued connections.** Reports maximum number of queued connections at any given time for reported period. **Average active connections.** Reports average number of active connections to I-Gear at any given time for reported period.
Cache Information	**Total items.** Reports total number of items contained in the cache at the time report is generated. **Memory used by the cache.** Reports system memory in megabytes used by the cache at the time report is generated. **Disk used by the cache.** Reports amount of disk space in megabytes used by the cache at the time report is generated. **Note:** The information contained in this portion (Cache Information) of the report is, by definition, not averaged for the entire period specified for the report but represents a snapshot of the cache at the time report is generated.



Gear
INTERNET CONTENT MANAGEMENT SOFTWARE

Cache Report

17-Feb-1999 08:00:00 - 17-Feb-1999 18:00:00

Request Summary

Cache Hits	126	(20.97%)
Cacheable Requests	345	(57.40%)
Uncacheable Requests	114	(18.97%)
Failed	16	(2.66%)
Total	601	

Data Transfer Summary

MBs Served from Cache	0.25 (7.83%)
MBs Served from Network	2.99 (92.17%)
Total	3.25 MB
Average Request Size	5.54 KB

Performance Summary

Time in seconds

	Average
Total Request Processing	1.11
Network Delay	1.06

User Session Summary

License Limit	29
Maximum Concurrent Usage	20
Average Concurrent Usage	16

Active Connection Summary

Current Simultaneous Connection Setting	15
Maximum Active Connections	4
Maximum Queued Connections	0
Average Active Connections	0

Cache Information

Run Began: 17-Feb-1999 09:55:12

Total Items	4672
Memory Used by Cache	2 MB
Disk Used by Cache	38 MB

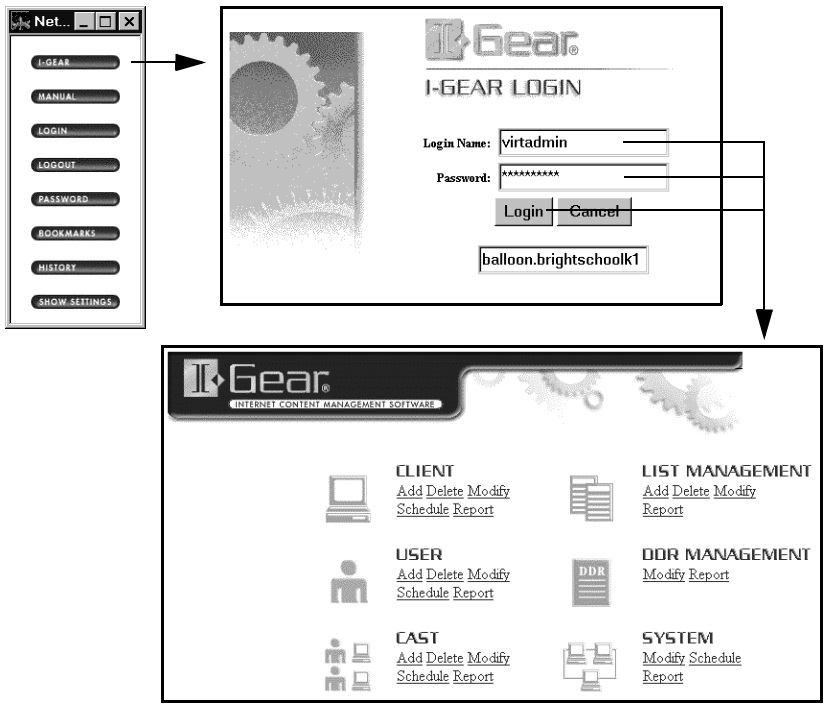
12. Using I-Gear: Some Examples

This section provides sample scenarios to help you maximize I-Gear's effectiveness. Although these scenarios involve specific settings, for example, library, school, or corporate environments, the information contained in the scenarios can be more generally applied.

Initial Setup (Configuring I-Gear)

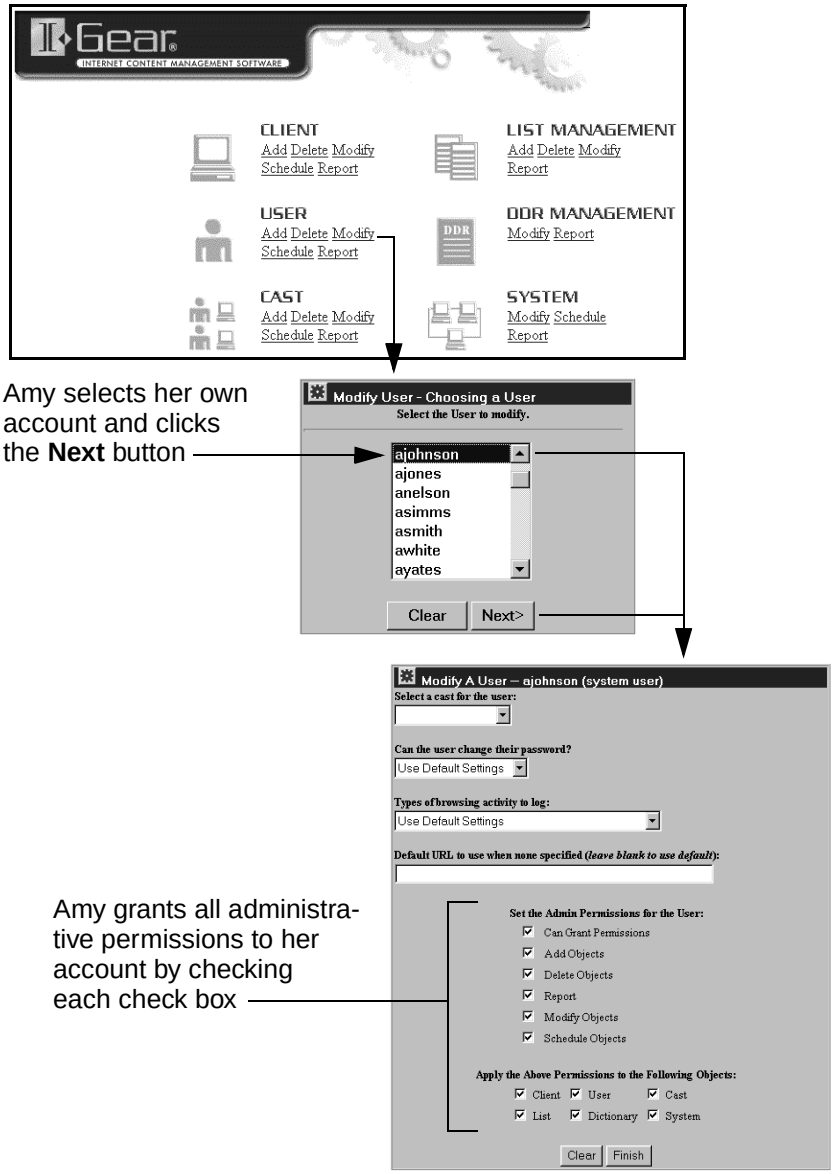
Brightschool has just purchased I-Gear. Amy is Brightschool's computer expert; her task is to configure I-Gear specifically for the school. She has installed I-Gear on the school's server and has followed carefully the instructions in the *I-Gear Installation Guide*. Thus, Amy already has accepted the default port number (8002) for I-Gear, set the cache size, obtained Brightschool's I-Gear license, and set the system defaults for basic filtering. Brightschool is not using transparent proxying, so she also has configured the Web browser of each Client computer to proxy through the server running I-Gear.

Brightschool's server is named `balloon`. Amy first accesses the I-Gear tool bar by visiting `http://balloon:8002/toolbar`.



She then accesses the I-Gear Administration page by clicking the **I-Gear** button on the tool bar and logging in as `virtadmin`. She uses the password she entered during the I-Gear installation.

Amy first wants to grant administrative permissions to her own account. She selects the Modify shortcut for the User object from the I-Gear administrative page.



She then selects her own account from the list of Users and clicks the **Next** button. By checking all of the check boxes shown on the next screen, Amy grants all administrative permissions to her account. She clicks the **Finish** button to save her changes.

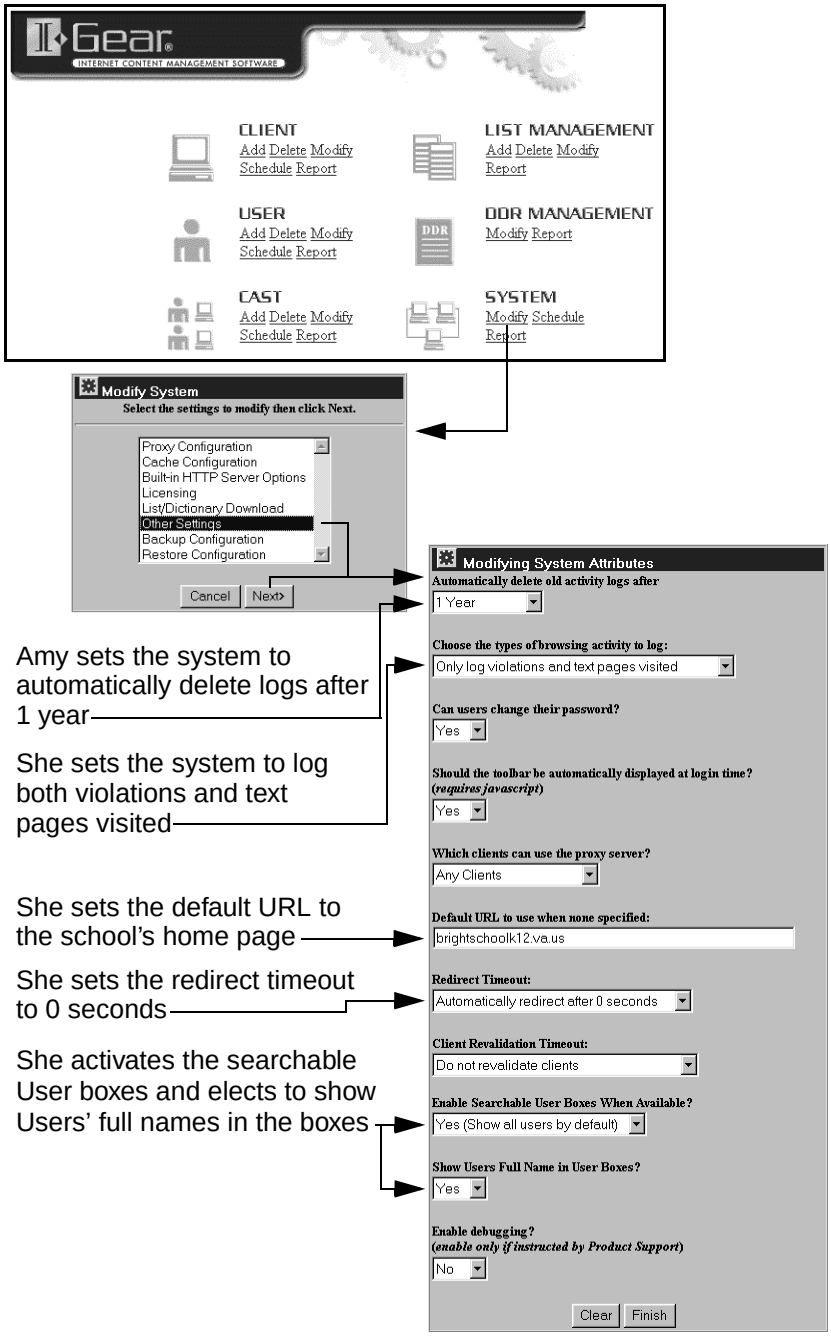
Now Amy could use her own account to administer I-Gear, but she decides to continue configuring I-Gear using the `virtadmin` account right now.

Amy next wants to customize the overall system settings. From the I-Gear Administration page, she selects the Modify shortcut for the System object. She then selects Other Settings from the menu provided and clicks the **Next** button.

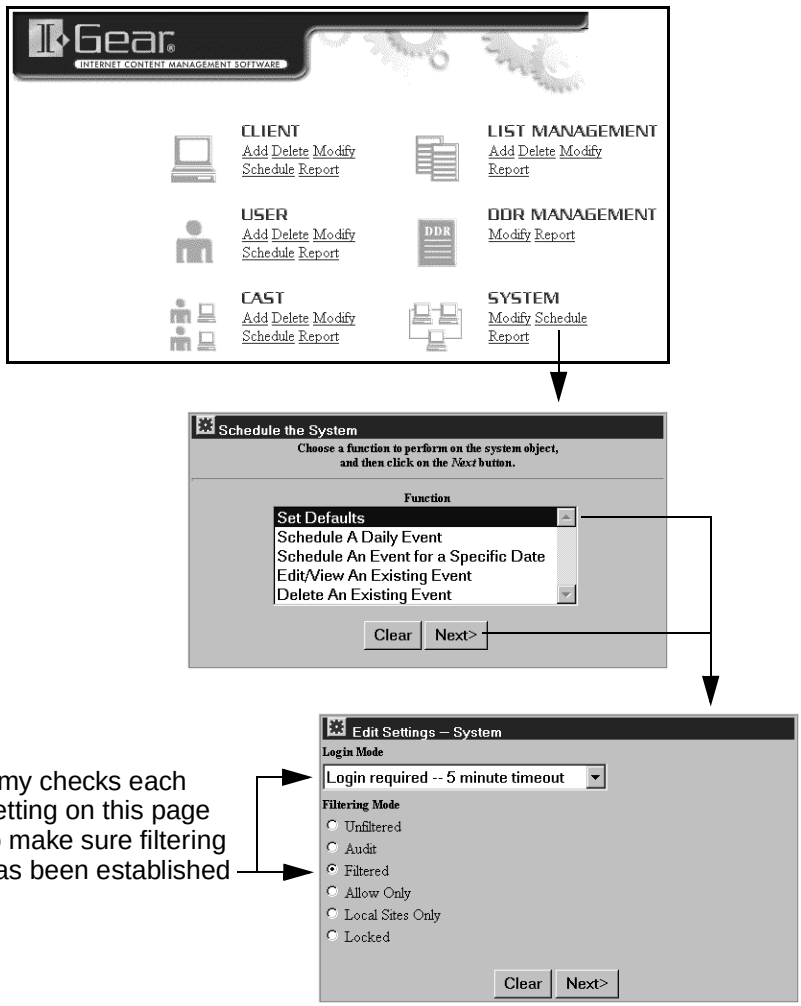
From the next display, Amy makes the following changes.

- The server has plenty of disk space, so Amy sets the system to remove log files automatically after 1 year. The log files are required in order for the reporting functions to work correctly, and Brightschool's policy does not require reporting on Internet accesses more than 1 year in the past.
- The school's policies require comprehensive reporting on Internet usage, so Amy specifies that browsing activity logs should include both text pages visited and violations.
- Amy sets the default URL to the school's home page. This URL will display when no other URL has been requested (e.g., after the I-Gear Login Complete page has finished displaying).
- All Client computers on the network support automatic refresh after login, so Amy sets the refresh time to 0 seconds so that the I-Gear Login Complete page appears only briefly after a successful login.
- The student population at Amy's school is fairly large, so Amy activates the searchable User boxes in I-Gear. Now whenever she needs to find a particular account in a list of Users she can use the search capability if necessary.
- Amy also elects to have Users' full names displayed beside the account names in User boxes so that she can easily identify account owners.

Amy leaves the other settings on this screen alone because the default settings for these options are acceptable. After making the necessary changes, she clicks the **Finish** button to save the changes.



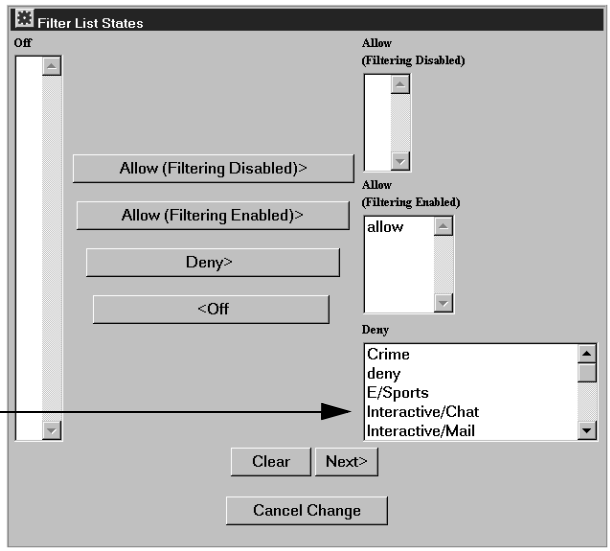
Amy next wants to verify the default filtering properties for her system, which she specified during installation in accordance with the instructions in the *I-Gear Installation Guide*. To check the system default settings, Amy returns to the I-Gear administration screen and selects the Schedule shortcut for the System object. From the next screen, she selects the Set Defaults option and clicks the **Next** button.



School policy requires Users to log in before accessing the Internet so that reports can be generated per User if necessary. Amy sees that "Login required--5 minute timeout" is selected. The school also wants filtering to be turned on by default. Amy also sees that Filtered is the default filtering setting. She clicks the **Next** button to check the settings on the next page.

The next screen shows the state of all predefined Content Category Lists. Amy checks to make sure that each List has been placed in the appropriate List state. That is, those Lists for which access is to be denied are in the Deny state, those for which access is to be allowed are in the appropriate Allow state, and those for which filtering is not to occur have been left in the Off state. Brightschool has very strict rules regarding the types of material that may be accessed over the Internet. To comply with those requirements, Amy makes sure that all predefined Content Category Lists have been moved to the Deny state (except the predefined List entitled "allow," which she leaves in the Allow (Filtering Enabled) state (the default state for this List)). After making sure that the predefined Content Category Lists are in the appropriate states, Amy selects the **Next** button to check the settings on the next page.

Amy then checks to make sure that all applicable lists have been moved to the Deny state



This next display covers other filtering options. The school only has a 28.8kbps modem connection to the Internet; therefore, Amy does not want to allow movies to be downloaded because movies tend to be large files and may tie up the modem connection. Thus, she checks to make sure that the check boxes for `mov...` and `mpeg...` have been selected under Block Extensions. She also makes sure that the check boxes for `zip` and `exe` files have been selected to prevent download of possible PC executable files. She also ensures that AutoLock has been enabled. She makes sure that the method for AutoLocking a User's account is a scheduled default event for the individual User. She also

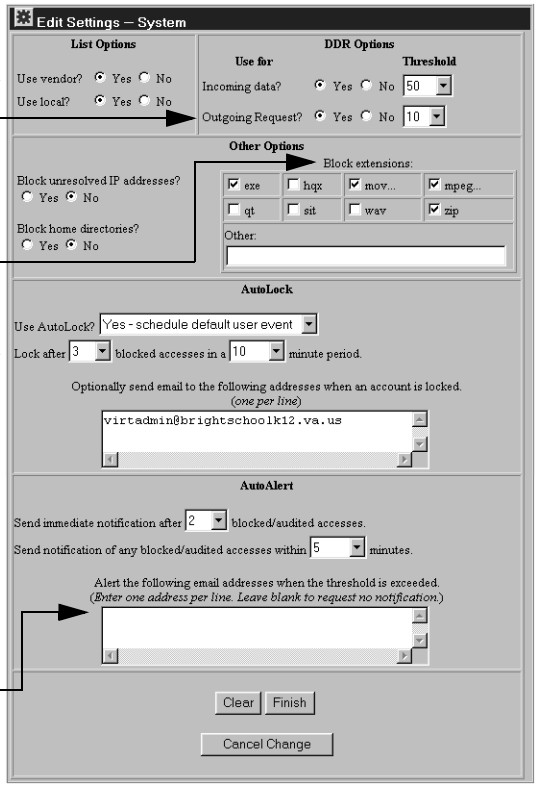
makes sure that AutoAlert is not active (i.e., the e-mail address field is blank) for now. Amy can activate AutoAlert later if necessary.

Amy makes sure that vendor and local lists are enabled and that DDR has been activated for both incoming data and outgoing requests

Amy makes sure that any extensions she wants blocked have been checked

She also makes sure that AutoLock has been enabled and that her e-mail address has been entered for AutoLock notification

Amy makes sure that AutoAlert has not been activated for now

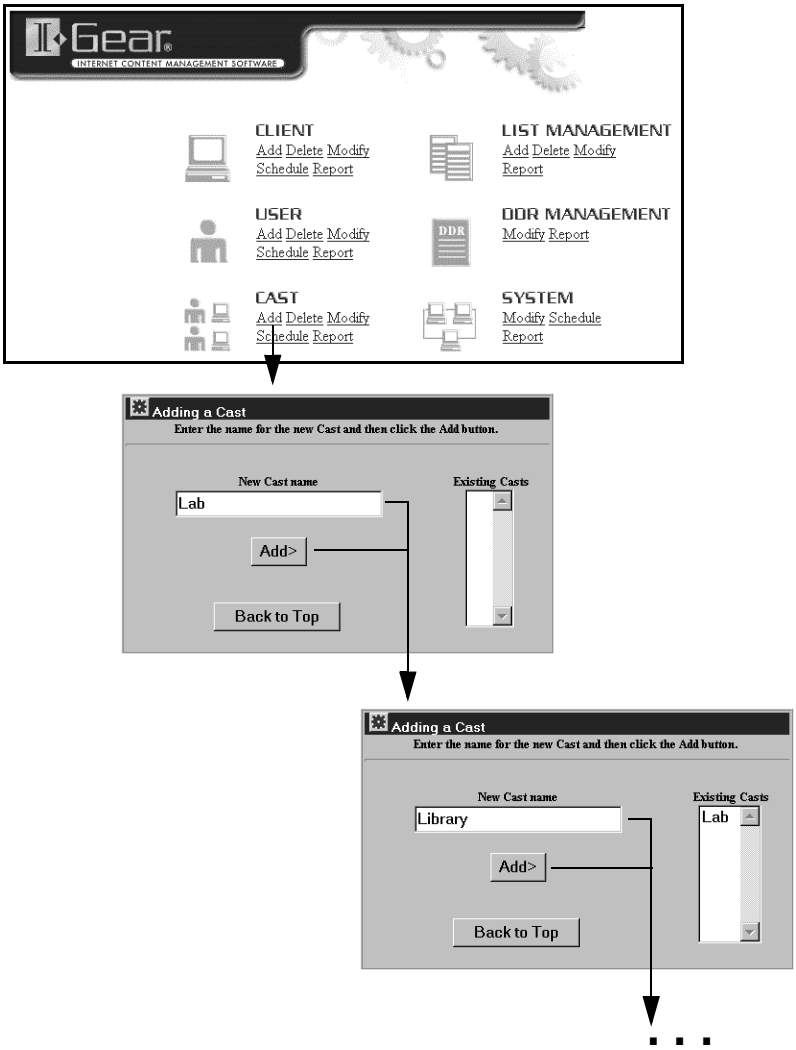


Now that Amy is assured that basic filtering has been established and that the System default settings are correct, she clicks the **Finish** button. (She could also click the **Cancel Change** button because she did not change any of the settings.)

Next, Amy wants to group related Clients together and related Users together into Casts so that she can easily schedule different filtering permissions for these Users or Clients later, if needed.

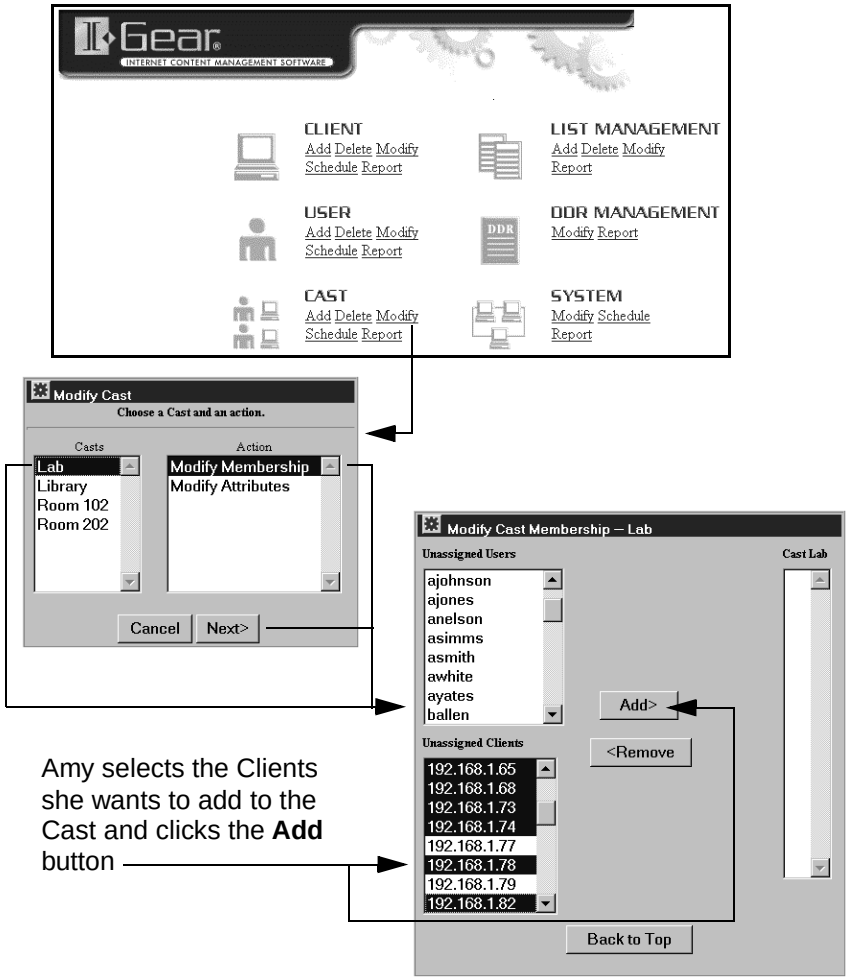
First she creates the (empty) Casts. She selects the Add shortcut for the Cast object from the I-Gear Administration page. She creates the following Casts for the Client computers: “Lab,” “Library,” “Room 102,” and “Room 202.” She creates each new Cast by entering the name of the

new Cast in the field provided and clicking the **Add** button. When she has finished creating new Casts, she clicks the **Back to Top** button.



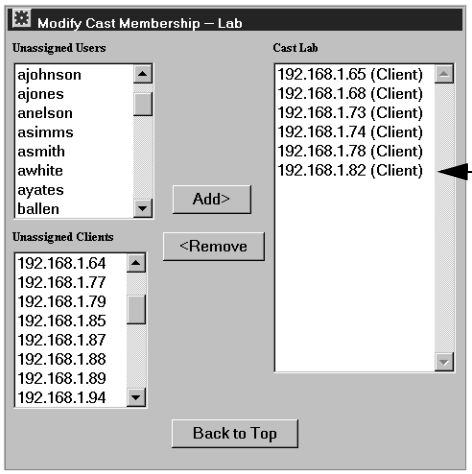
Amy then proceeds to modify the membership of each Cast to include the appropriate Client objects. She first selects the Modify shortcut for the Cast object. From the next display, she selects the Cast she wants to modify, selects the Modify Membership function, and clicks the **Next** button. From the next display, Amy selects the Client objects to populate

that Cast. When she has selected the appropriate Clients, she clicks the **Add** button.



The selected Clients are then shown on the right side of the display as Client members of the modified Cast.

Amy then repeats these steps for each new Client Cast.

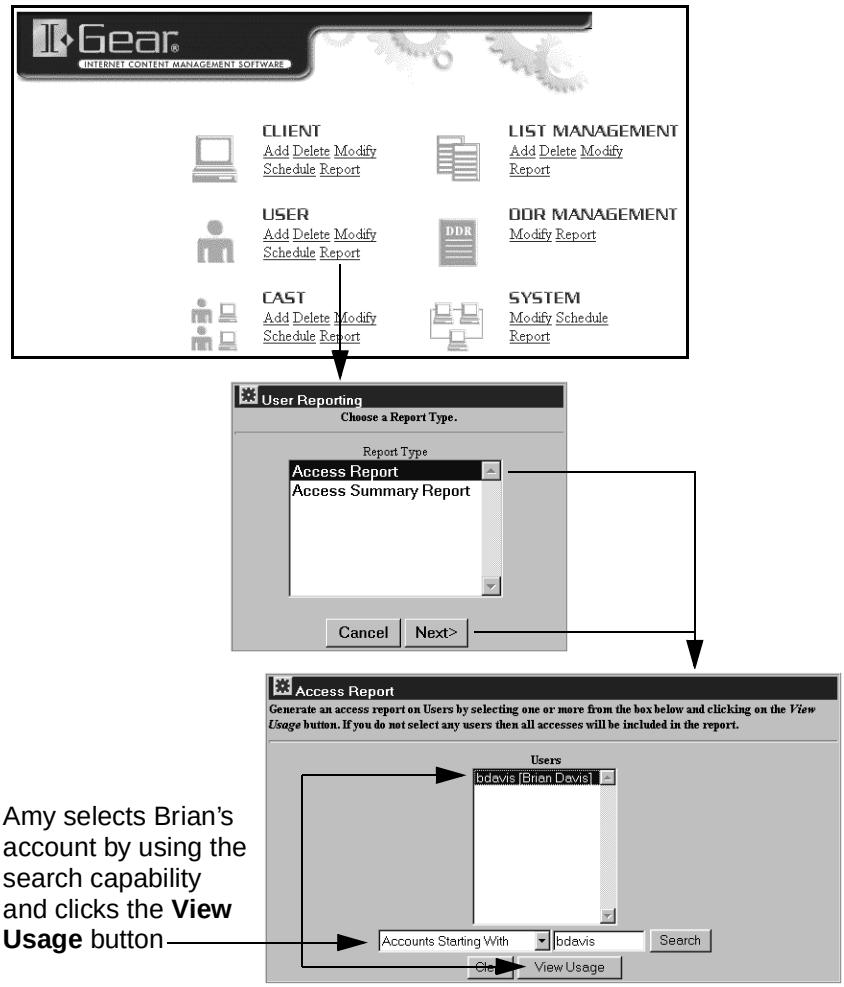


The added Clients now appear as members of the Cast

After she has populated all Client Casts with the appropriate Client objects, Amy repeats the steps for creating and modifying Casts for Users. Once she has completed creating and populating User Casts, Amy decides she is finished customizing I-Gear for now.

Automated Policy Enforcement (Using AutoLock)

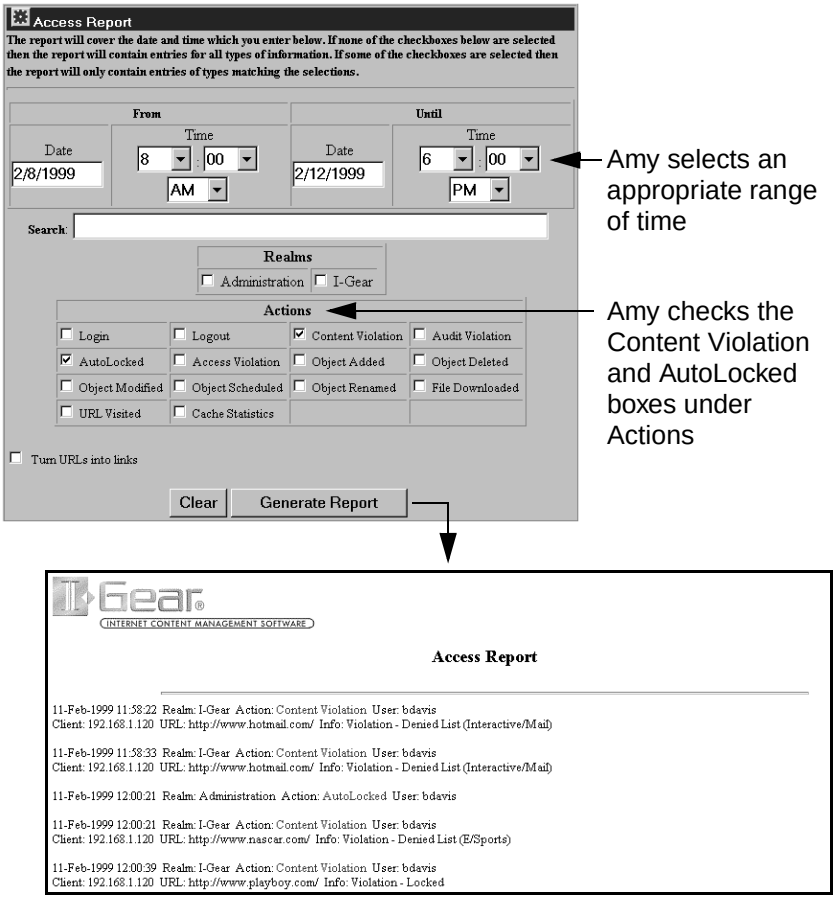
Amy (the school's computer expert) receives an e-mail message from I-Gear informing her that Brian's (a student at Brightschool) account is locked. Amy accesses the I-Gear administration screen and selects the Report shortcut for the User object. She then selects Access Report and clicks the **Next** button. From the next screen, she selects Brian's account and clicks the **View Usage** button.



Amy selects Brian's account by using the search capability and clicks the **View Usage** button

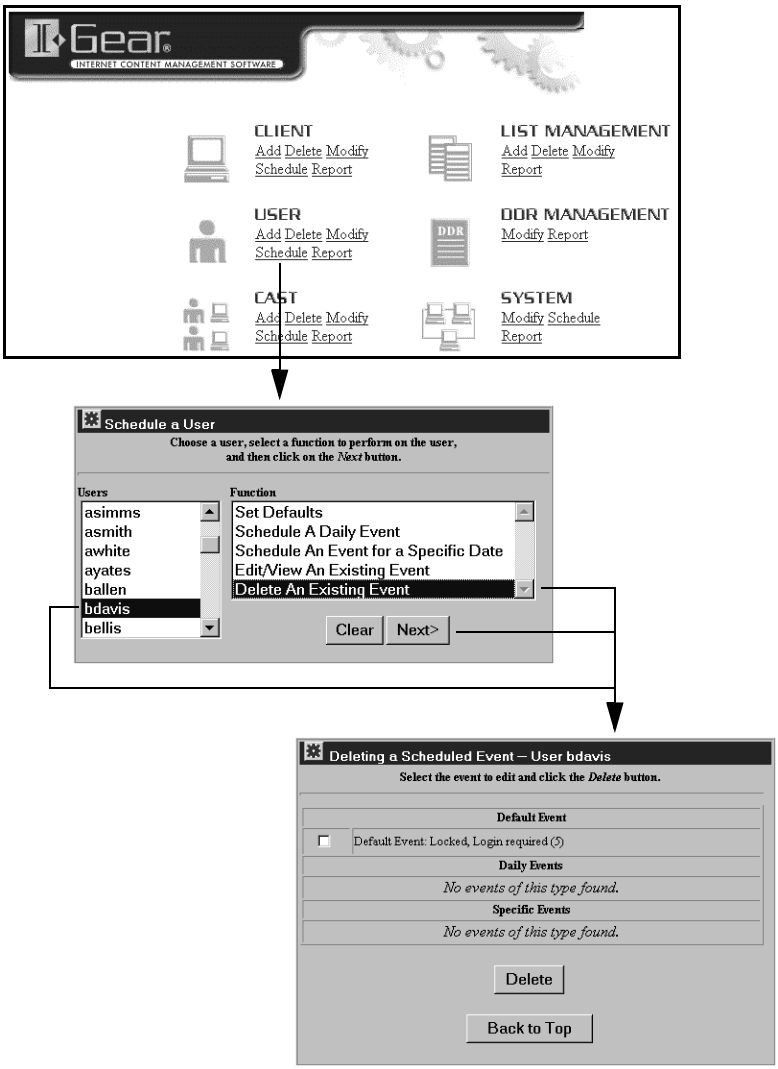
Next, Amy needs to select a time range for the report. She enters a range that covers the previous week. She clicks the check boxes for Content Violations and AutoLocked under Actions because those actions are all she needs to see right now. She clicks the **Generate Report** button. As

Amy suspected, Brian has tried to visit several sites that the school has determined to be inappropriate. A recent administrative entry shows that Brian's account was AutoLocked, which means that Brian's default filtering settings have been set to Locked automatically.


Access Report
The report will cover the date and time which you enter below. If none of the checkboxes below are selected then the report will contain entries for all types of information. If some of the checkboxes are selected then the report will only contain entries of types matching the selections.
From
Until
Time
Date
2/8/1999
8
00
AM
2/12/1999
6
00
PM
Search:
Realms
Administration
I-Gear
Actions
Login
Logout
Content Violation
Audit Violation
AutoLocked
Access Violation
Object Added
Object Deleted
Object Modified
Object Scheduled
Object Renamed
File Downloaded
URL Visited
Cache Statistics
Turn URLs into links
Clear
Generate Report
Amy selects an appropriate range of time
Amy checks the Content Violation and AutoLocked boxes under Actions
I-Gear
INTERNET CONTENT MANAGEMENT SOFTWARE
Access Report
11-Feb-1999 11:58:22 Realm: I-Gear Action: Content Violation User: bdavis
Client: 192.168.1.120 URL: http://www.hotmail.com/ Info: Violation - Denied List (Interactive/Mail)
11-Feb-1999 11:58:33 Realm: I-Gear Action: Content Violation User: bdavis
Client: 192.168.1.120 URL: http://www.hotmail.com/ Info: Violation - Denied List (Interactive/Mail)
11-Feb-1999 12:00:21 Realm: Administration Action: AutoLocked User: bdavis
11-Feb-1999 12:00:21 Realm: I-Gear Action: Content Violation User: bdavis
Client: 192.168.1.120 URL: http://www.nascar.com/ Info: Violation - Denied List (E/Sports)
11-Feb-1999 12:00:39 Realm: I-Gear Action: Content Violation User: bdavis
Client: 192.168.1.120 URL: http://www.playboy.com/ Info: Violation - Locked

Amy could unlock Brian's account by selecting the Schedule shortcut for the User object and then selecting Brian's account and the Delete an Existing Event function. All events scheduled for Brian (including his default setting, which is Locked) are displayed on the next screen. From this display, Amy could delete the default setting. Or if specific default settings had been established for Brian, Amy could select the Set

Defaults function and change the filtering mode from Locked back to the appropriate settings.

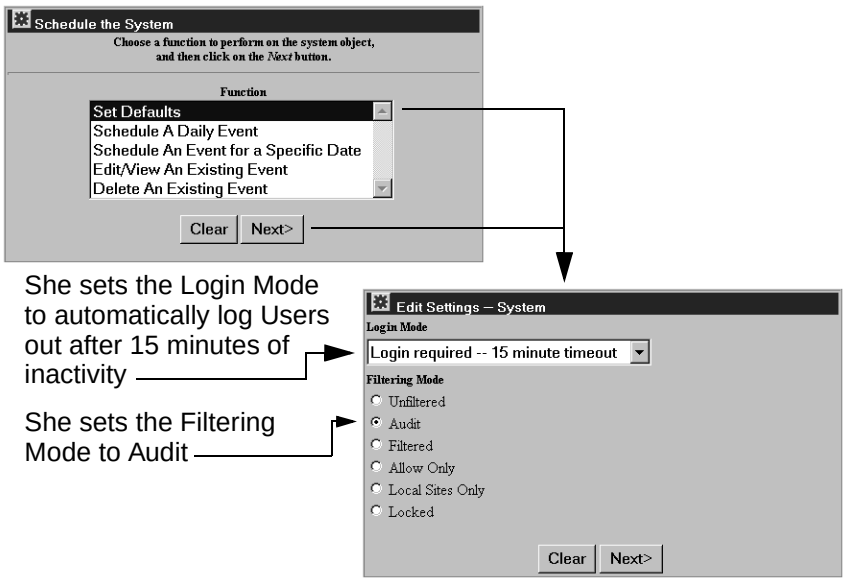


However, school policy dictates that Brian must have a letter signed by his parents before his Internet access can be restored, so Amy leaves his default settings alone for now.

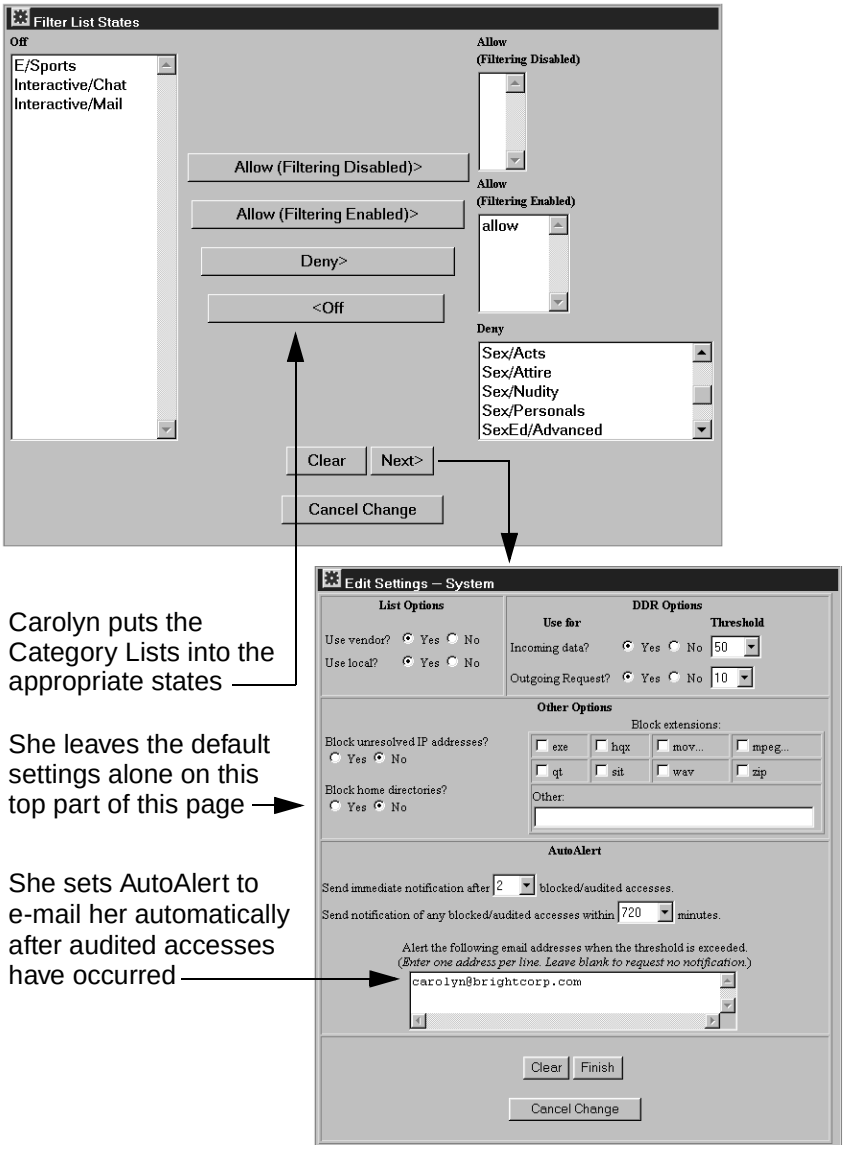
Monitoring Internet Access (Using Audit Mode and AutoAlert)

Carolyn is the manager and owner of a small but growing company. Her business depends on employees being able to use the Internet regularly. She doesn't want to restrict her employees' access to the Internet; she feels that providing unrestricted access to the Internet as a resource is an important benefit to her employees and establishes a level of trust between her and her staff. However, she has concerns that one or two individuals may be abusing this privilege during work hours. She decides to run I-Gear in Audit Mode for a while to see whether her suspicions are correct. In Audit Mode, employees have unrestricted access, and Carolyn, with I-Gear's AutoAlert feature, will be notified when violations of her Internet use policy have occurred. By using Access Reporting, she can see exactly where these violations occurred.

Carolyn first schedules the System defaults to Audit Mode and activates AutoAlert. Because Carolyn has just purchased I-Gear, setting the System defaults to Audit Mode is all she needs to do. If her company had been using the software for a while, Carolyn would need to make sure that no other events override the System defaults. To set the System defaults, she selects the Schedule shortcut for the System object. She then selects the Set Defaults function and clicks the **Next** button. From the next screen, she selects the login mode to automatically log Users out after 15 minutes of inactivity and selects Audit as the filtering mode. She then clicks the **Next** button.



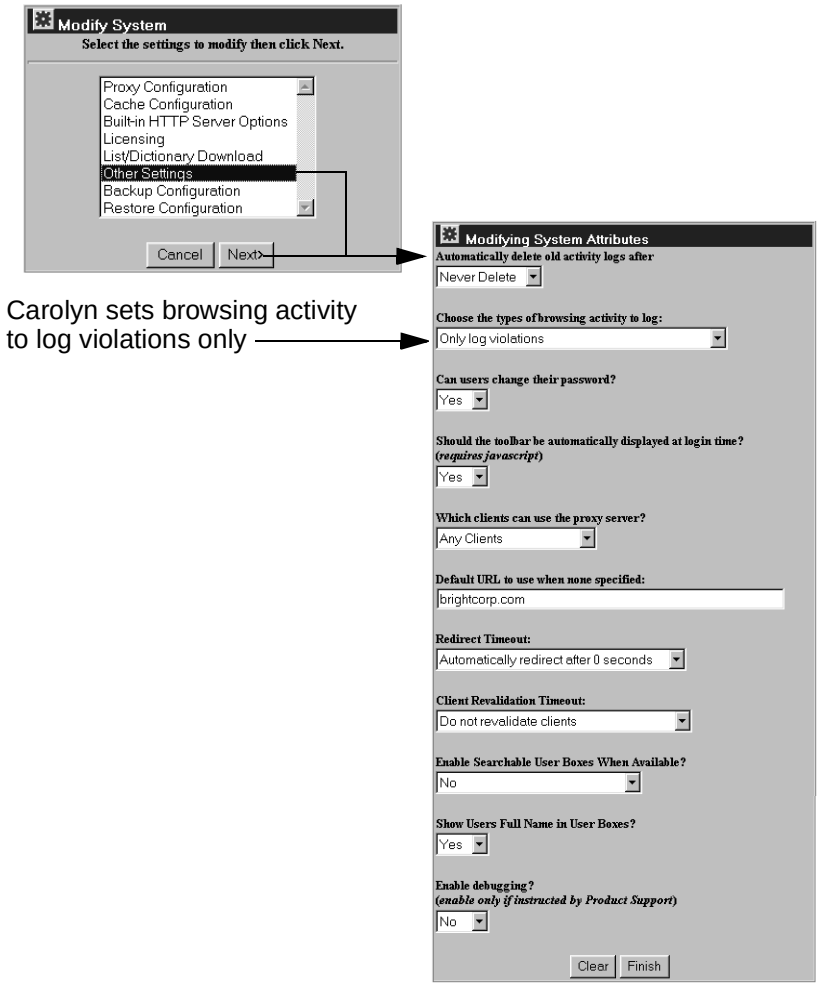
From the next screen, she selects the Content Category Lists that contain material she would consider objectionable during work hours and moves them into the Deny state. She leaves several Content Category Lists in the Off state because she does not want to filter the type of content contained in those lists. After she places the Content Category Lists in the appropriate states, she again clicks the **Next** button.



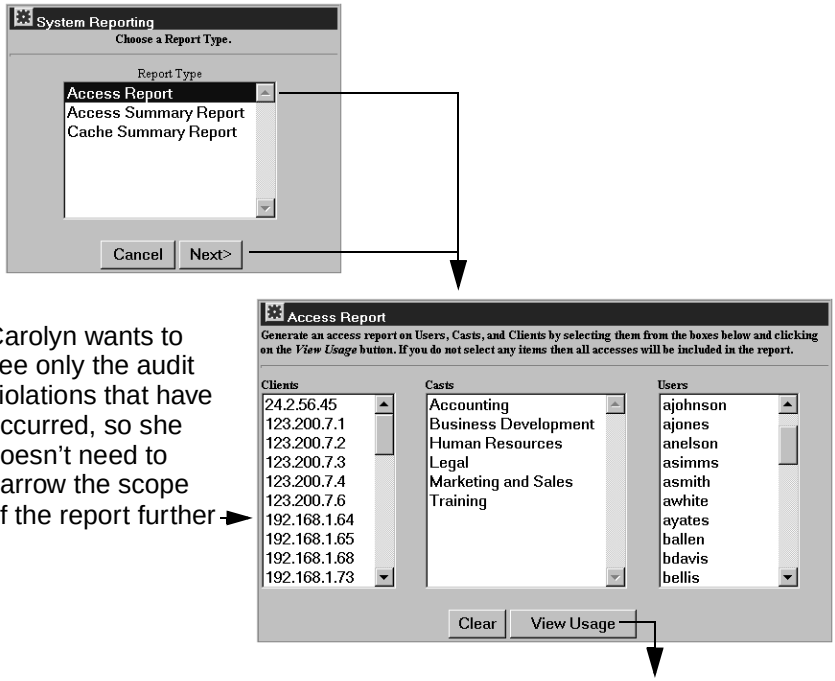
She leaves the filtering settings on the next page alone. She is confident that the default settings will be adequate for what she wants to know.

She enters her own e-mail address in the field provided for AutoAlert notification, so that I-Gear will notify her of any access violations that occur. She also sets the other parameters for AutoAlert to appropriate settings.

Carolyn next sets I-Gear's activity logging to log violations only. She does not want to pry unnecessarily into how her employees use the Internet; she only wants to know when a content violation based on her acceptable-use policy has occurred. She selects the Modify shortcut for the System object. From the next screen, she selects the Other Settings function and clicks the **Next** button. From the next screen, she sets browsing activity logging to Only Log Violations. She then clicks the **Finish** button.



Carolyn has finished setting up Audit Mode. Now she simply has to wait to see if she receives any e-mail indicating that content violations have occurred. Over the next two weeks, she receives several e-mail messages from I-Gear indicating that two different employees have violated the acceptable-use policy. Carolyn has a few minutes and decides to run an Access Report to get a full report. She first selects the Report shortcut for the System object. From the next screen, she selects Access Report and clicks the **Next** button. From this screen, she could select certain Users, Clients, or Casts on which to report. However, because she wants to view only the audit violations that have occurred, she doesn't need to worry about narrowing the scope of the report further. She then clicks the **View Usage** button.



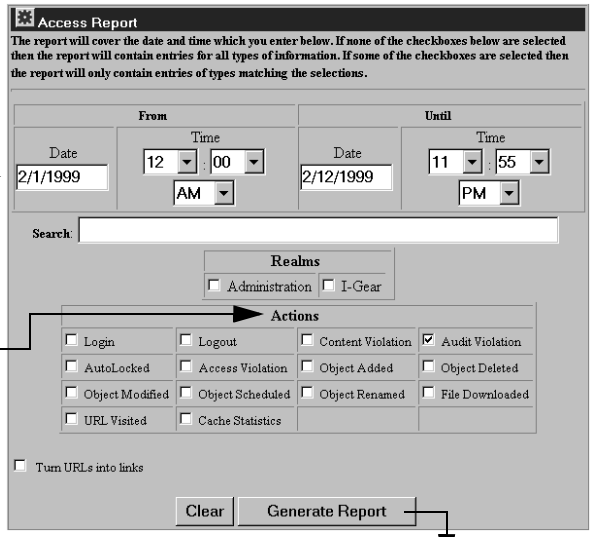
Carolyn wants to see only the audit violations that have occurred, so she doesn't need to narrow the scope of the report further

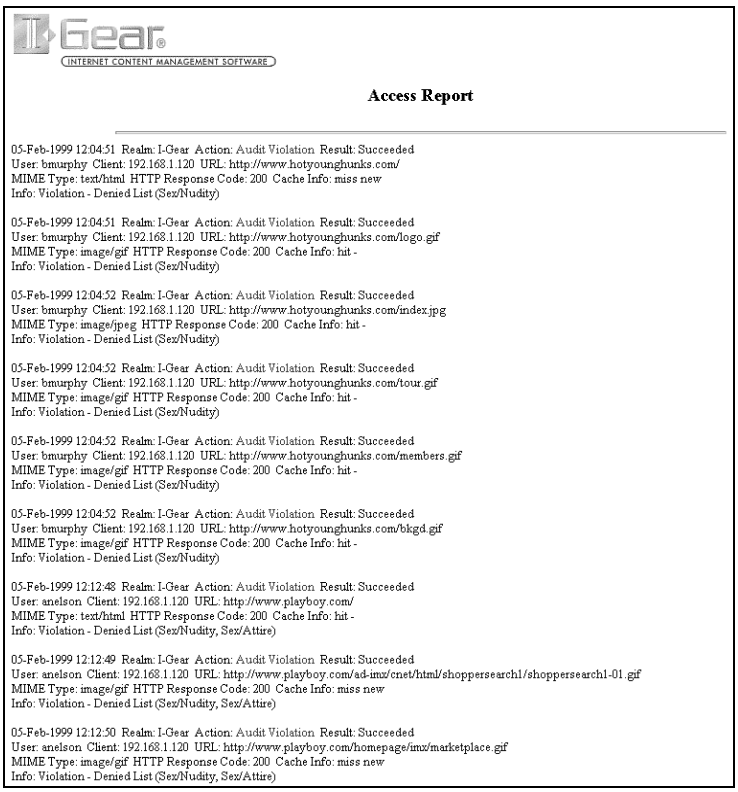
From the next screen, she selects the dates and times she wants to cover in the report. She enters a range that covers the previous two weeks. For this report, Carolyn is only interested in the Audit Violations that have

occurred, so she checks only that check box under Actions. She then clicks the **Generate Report** button.

She selects the dates and times to be covered by the report

She selects the appropriate action on which to report (in this case, only Audit Violations)





Gear
INTERNET CONTENT MANAGEMENT SOFTWARE

Access Report

05-Feb-1999 12:04:51 Realm: I-Gear Action: Audit Violation Result: Succeeded
User: bmurphy Client: 192.168.1.120 URL: http://www.hotyounghunks.com/
MIME Type: text/html HTTP Response Code: 200 Cache Info: miss new
Info: Violation - Denied List (Sex/Nudity)

05-Feb-1999 12:04:51 Realm: I-Gear Action: Audit Violation Result: Succeeded
User: bmurphy Client: 192.168.1.120 URL: http://www.hotyounghunks.com/logo.gif
MIME Type: image/gif HTTP Response Code: 200 Cache Info: hit -
Info: Violation - Denied List (Sex/Nudity)

05-Feb-1999 12:04:52 Realm: I-Gear Action: Audit Violation Result: Succeeded
User: bmurphy Client: 192.168.1.120 URL: http://www.hotyounghunks.com/index.jpg
MIME Type: image/jpeg HTTP Response Code: 200 Cache Info: hit -
Info: Violation - Denied List (Sex/Nudity)

05-Feb-1999 12:04:52 Realm: I-Gear Action: Audit Violation Result: Succeeded
User: bmurphy Client: 192.168.1.120 URL: http://www.hotyounghunks.com/tour.gif
MIME Type: image/gif HTTP Response Code: 200 Cache Info: hit -
Info: Violation - Denied List (Sex/Nudity)

05-Feb-1999 12:04:52 Realm: I-Gear Action: Audit Violation Result: Succeeded
User: bmurphy Client: 192.168.1.120 URL: http://www.hotyounghunks.com/members.gif
MIME Type: image/gif HTTP Response Code: 200 Cache Info: hit -
Info: Violation - Denied List (Sex/Nudity)

05-Feb-1999 12:04:52 Realm: I-Gear Action: Audit Violation Result: Succeeded
User: bmurphy Client: 192.168.1.120 URL: http://www.hotyounghunks.com/bkgd.gif
MIME Type: image/gif HTTP Response Code: 200 Cache Info: hit -
Info: Violation - Denied List (Sex/Nudity)

05-Feb-1999 12:12:48 Realm: I-Gear Action: Audit Violation Result: Succeeded
User: anelson Client: 192.168.1.120 URL: http://www.playboy.com/
MIME Type: text/html HTTP Response Code: 200 Cache Info: hit -
Info: Violation - Denied List (Sex/Nudity, Sex/Attire)

05-Feb-1999 12:12:49 Realm: I-Gear Action: Audit Violation Result: Succeeded
User: anelson Client: 192.168.1.120 URL: http://www.playboy.com/ad-imx/cnet/html/shoppersearch1/shoppersearch1-01.gif
MIME Type: image/gif HTTP Response Code: 200 Cache Info: miss new
Info: Violation - Denied List (Sex/Nudity, Sex/Attire)

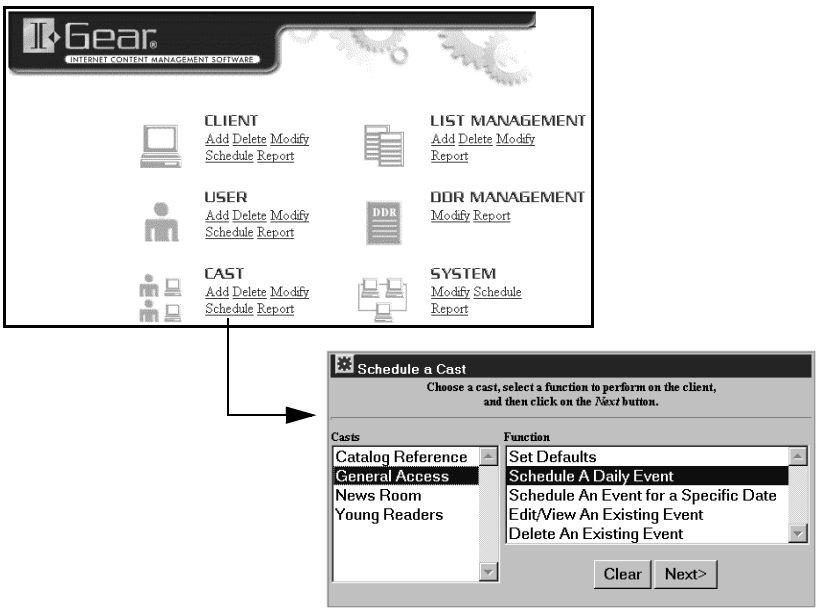
05-Feb-1999 12:12:50 Realm: I-Gear Action: Audit Violation Result: Succeeded
User: anelson Client: 192.168.1.120 URL: http://www.playboy.com/homepage/imx/marketplace.gif
MIME Type: image/gif HTTP Response Code: 200 Cache Info: miss new
Info: Violation - Denied List (Sex/Nudity, Sex/Attire)

Carolyn's Access Report shows her all audit violations that occurred in the previous two-week period. The violations were indeed committed by the two employees reported by AutoAlert: A. Nelson and B. Murphy. The report shows Carolyn, for each Audit violation, the User who requested the Internet access, the Client workstation used, the date and time of the request, the URL that was visited, and the reason that I-Gear would have denied access to the site had filtering actually been activated. With this documented evidence of policy violations by employees Nelson and Murphy, Carolyn is able to take appropriate measures.

Controlling Access (Scheduling Daily Events)

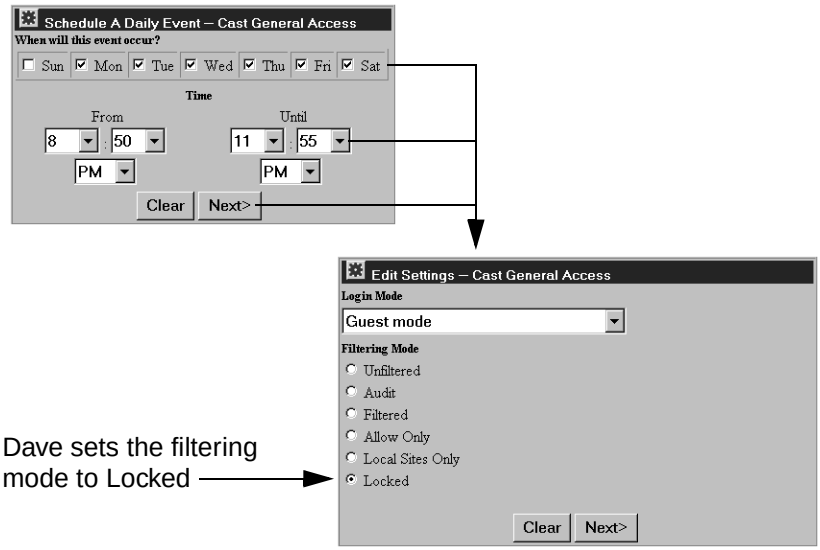
The Dane County Public Library has selected I-Gear to meet its access control needs. The library uses I-Gear's scheduling capabilities to provide an appropriate level of filtering in the children's areas and less restricted Internet access in other parts of the library. Thus, the library can avoid the problem of overbroad, unconstitutional restriction of Internet materials yet protect children from potentially harmful materials on the Internet.

The main branch of the library closes at 9 PM Monday through Saturday. However, patrons have a tendency to linger, browsing the Internet well past closing time. Thus, library employees have a difficult time closing the library and leaving on time. Dave, the system administrator for the library's computer network, decides to correct this problem by locking the library computers just prior to closing time. The library's computers are grouped into four Casts according to where they are located in the library: News Room, Young Readers, General Access, and Catalog Reference. Dave decides that he needs to lock the computers in all areas of the library except the Catalog Reference area, because those computers are right beside the front desk. Dave selects the Schedule shortcut for the Cast object. He then selects the "General Access" Cast and the Schedule a Daily Event function and clicks the **Next** button.



From the next screen, he selects Monday through Saturday and sets the time range from 8:50 PM to 11:55 PM. On the next page he does not change the Login mode (he leaves that setting on Guest Mode) and sets the filtering mode to Locked. He then clicks the **Next** button. I-Gear confirms that the changes have been made.

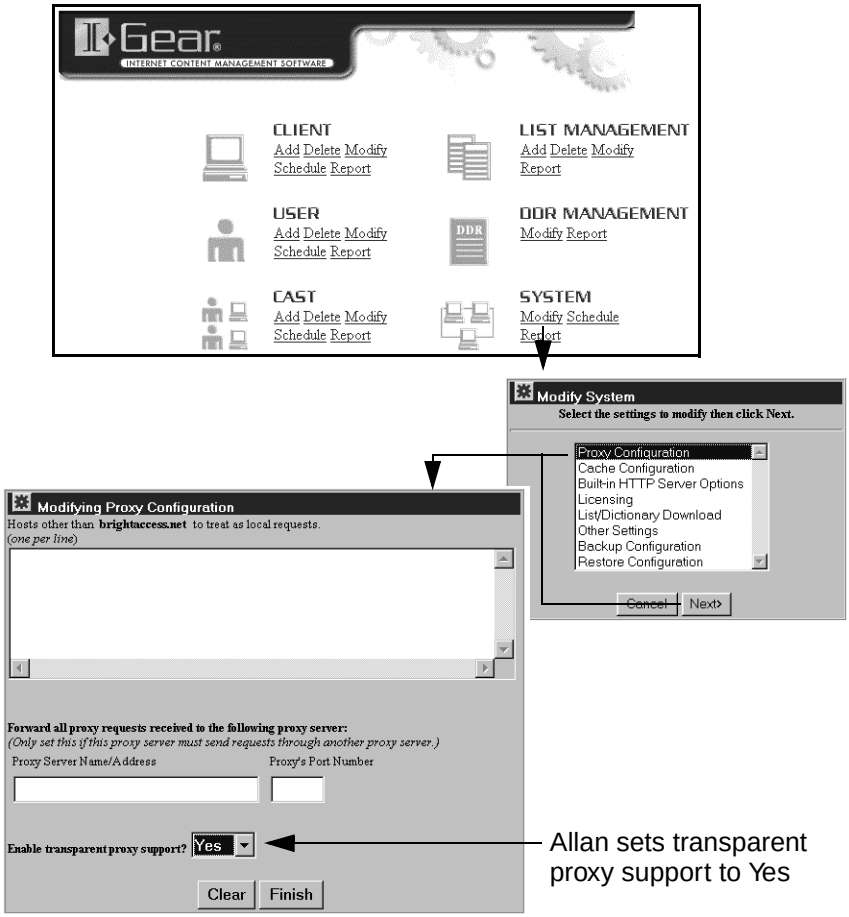
Dave then schedules identical daily events for the computers in the Young Readers and News Room Casts. Now, Monday through Saturday at 8:50 PM, the Client computers in the Young Readers, News Room, and General Access areas of the library will lock and will not permit access to the Internet.



ISP Configuration (Setting Up Transparent Proxying, Client Revalidation, and Casts)

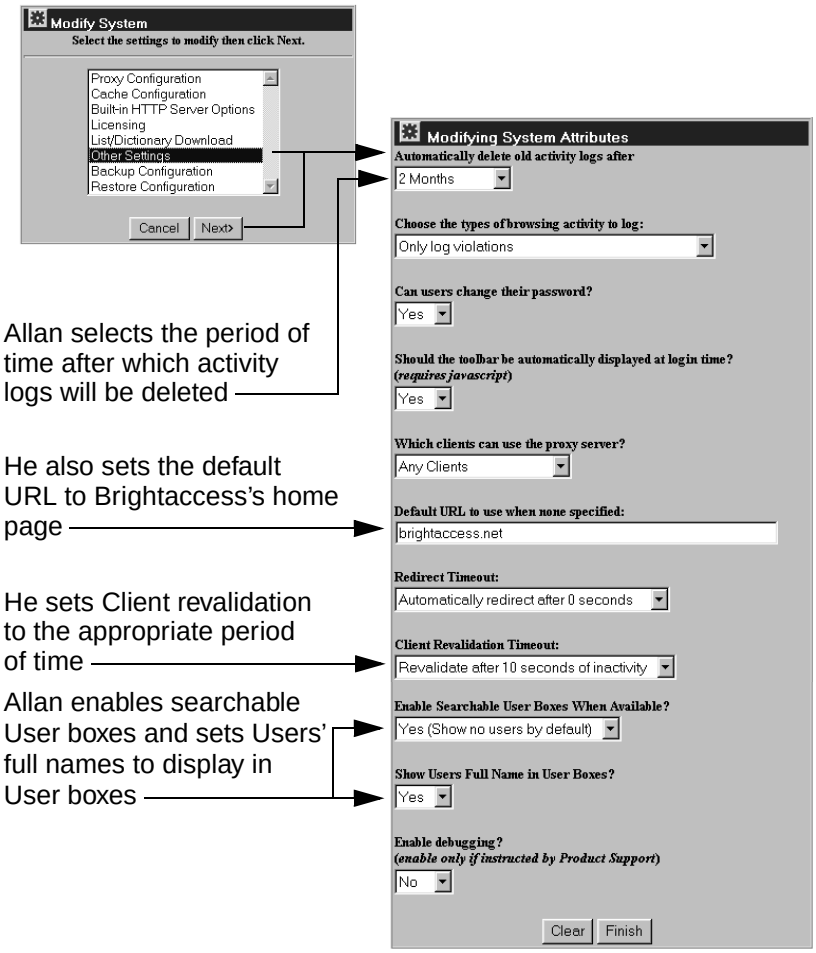
Allan is a systems administrator for a new Internet service provider (ISP), Brightaccess.net. Brightaccess has selected I-Gear so that they can offer customizable filtering options as part of their service to their subscribers. Allan has been put in charge of configuring I-Gear.

Brightaccess uses a transparent proxy setup. That is, Brightaccess's network has been configured to transparently proxy all HTTP requests through the server that is running I-Gear. Thus, Allan first must enable transparent proxy support in I-Gear. To enable transparent proxy support, Allan selects the Modify shortcut for the System object. From the next screen, he selects Proxy Configuration from the menu provided and then clicks the **Next** button. He then enables transparent proxy support by selecting Yes and clicking the **Finish** button.



Next, Allan must enable client revalidation. Allan knows that client revalidation is recommended for I-Gear in situations in which IP addresses are dynamically assigned to users as needed. (This scenario is typical in an ISP configuration.) Allan needs to activate this feature because different subscribers will have different levels of filtering and he wants to guard against a second User (having received the same IP address as an earlier user) being able to browse under the first User's filtering permissions if the first User does not log out of I-Gear properly. Allan can select the appropriate period of inactivity after which I-Gear will challenge a Client browser for a cookie automatically to ensure that the User has not changed.

To enable client revalidation, Allan selects the Modify shortcut for the System object. From the next screen, he selects Other Settings from the menu and clicks the **Next** button.


Modify System
Select the settings to modify then click Next.
Proxy Configuration
Cache Configuration
Built-in HTTP Server Options
Licensing
List/Dictionary Download
Other Settings
Backup Configuration
Restore Configuration
Cancel
Next>
Modifying System Attributes
Automatically delete old activity logs after
2 Months
Choose the types of browsing activity to log:
Only log violations
Can users change their password?
Yes
Should the toolbar be automatically displayed at login time?
(requires javascript)
Yes
Which clients can use the proxy server?
Any Clients
Default URL to use when none specified:
brightaccess.net
Redirect Timeout:
Automatically redirect after 0 seconds
Client Revalidation Timeout:
Revalidate after 10 seconds of inactivity
Enable Searchable User Boxes When Available?
Yes (Show no users by default)
Show Users Full Name in User Boxes?
Yes
Enable debugging?
(enable only if instructed by Product Support)
No
Clear
Finish
Allan selects the period of time after which activity logs will be deleted
He also sets the default URL to Brightaccess's home page
He sets Client revalidation to the appropriate period of time
Allan enables searchable User boxes and sets Users' full names to display in User boxes

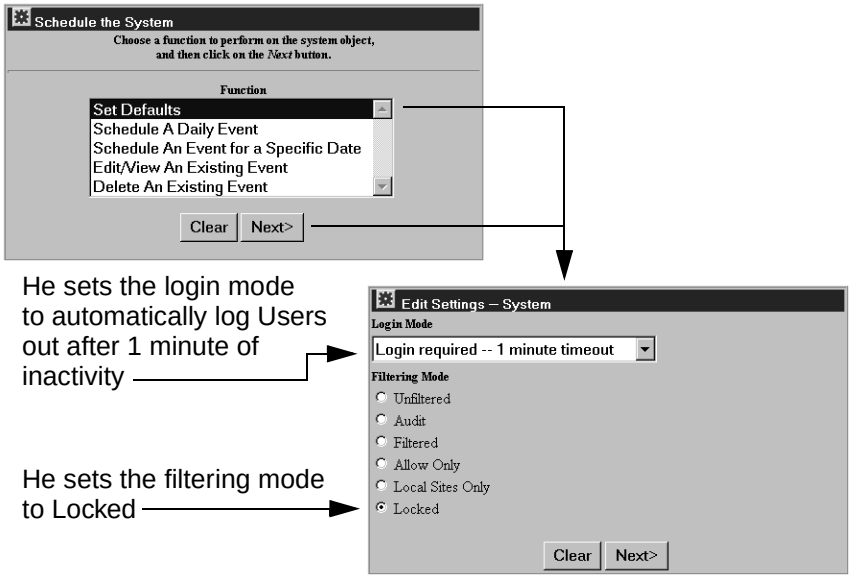
He selects the appropriate period of inactivity after which I-Gear will require client revalidation—Brightaccess has agreed that 10 seconds is an acceptable period of time for preventing one customer from accidentally being able to browse under another customer's permissions.

While he is changing the settings on this screen, Allan also sets the period of time that activity logs will be maintained on the system. Because of the available disk space and the expected level of browsing activity, he initially sets this period of time to 2 months. He can adjust this time period later, if necessary. He then sets the default URL that I-Gear will use when none has been specified by the customer to Brightaccess's home page. Allan then enables searchable User boxes (with no Users shown by default), and sets Users' full names to display in the User boxes. He is finished with the settings on this display, so he clicks the **Finish** button.

Now Allan needs to create the necessary Casts to support the different levels of filtering that Brightaccess will offer its subscribers. Brightaccess plans to use three levels of filtering: highly restrictive (suitable for young children), moderately restrictive (suitable for older children), and unfiltered (for adults). Brightaccess also plans to offer their subscribers a lower cost option for Internet access--for a lower monthly rate, subscribers can have unfiltered access but can access the Internet only during off-peak hours (12:00 AM to 8:00 AM).

To support the above Casts and the differing permissions, Allan must set the System defaults to Locked and schedule the permissions for each Cast. To set the System defaults, Allan selects the Schedule shortcut for

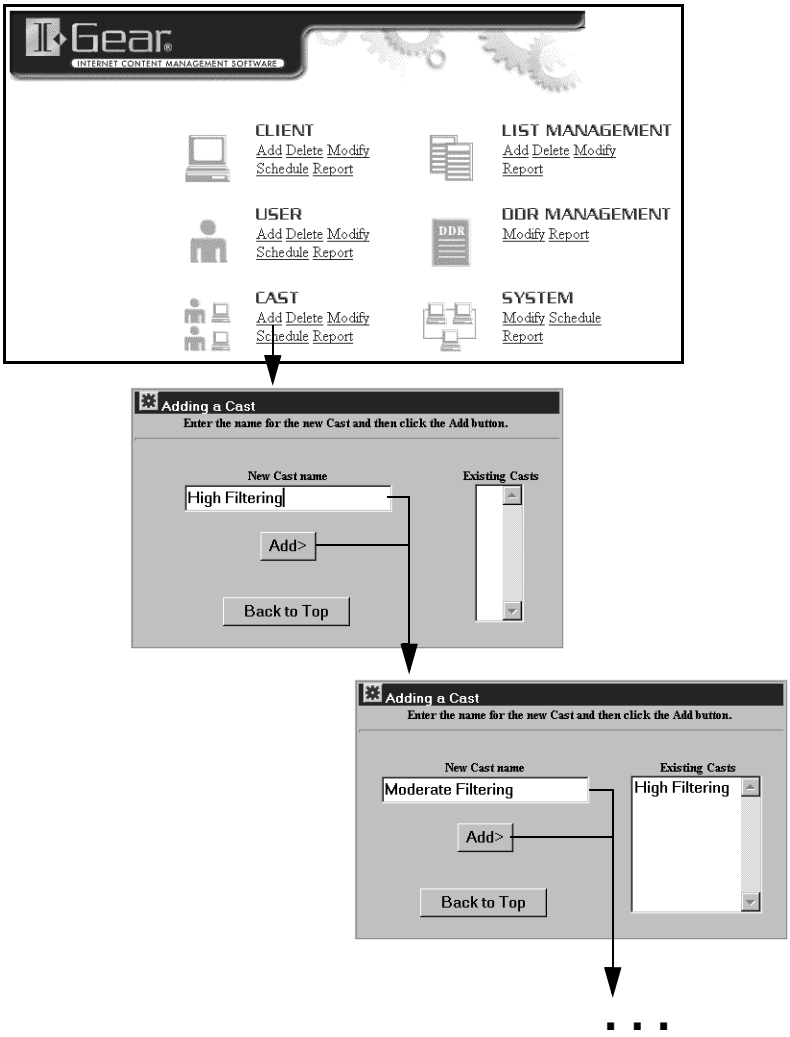
the System object. He selects the Set Defaults function, and clicks the **Next** button.



From the next screen, he selects the login mode to automatically log Users out after 1 minute of inactivity (so that a User who accidently logs in to I-Gear at a time when access is not permitted and does not log off properly will not tie up a session for a long period of time) and selects Locked as the filtering mode. He then clicks the **Next** button. I-Gear confirms that Allan's changes have been made.

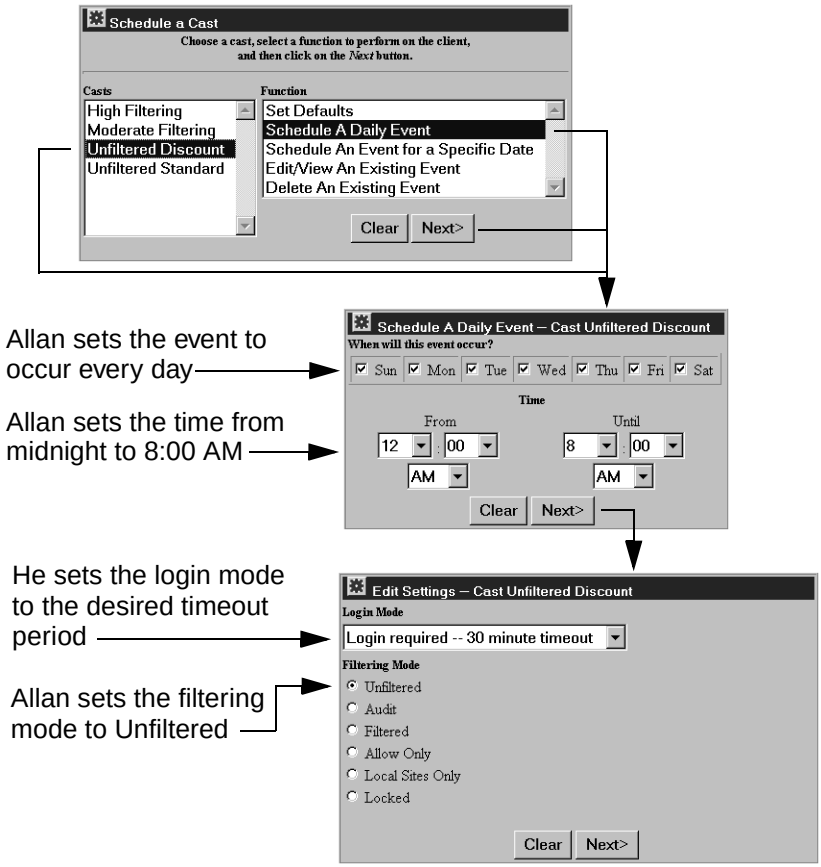
Allan is finished setting the System defaults. Now he must create the (empty) Casts he needs to establish the filtering levels. He creates four casts: High Filtering, Moderate Filtering, Unfiltered Standard, and Unfiltered Discount. To create the Casts, he selects the Add shortcut for the Cast object. From the next display, he creates each new Cast by entering the name of the new Cast in the field provided and clicking the

Add button. After Allan finishes creating the new Casts, he clicks the **Back to Top** button.



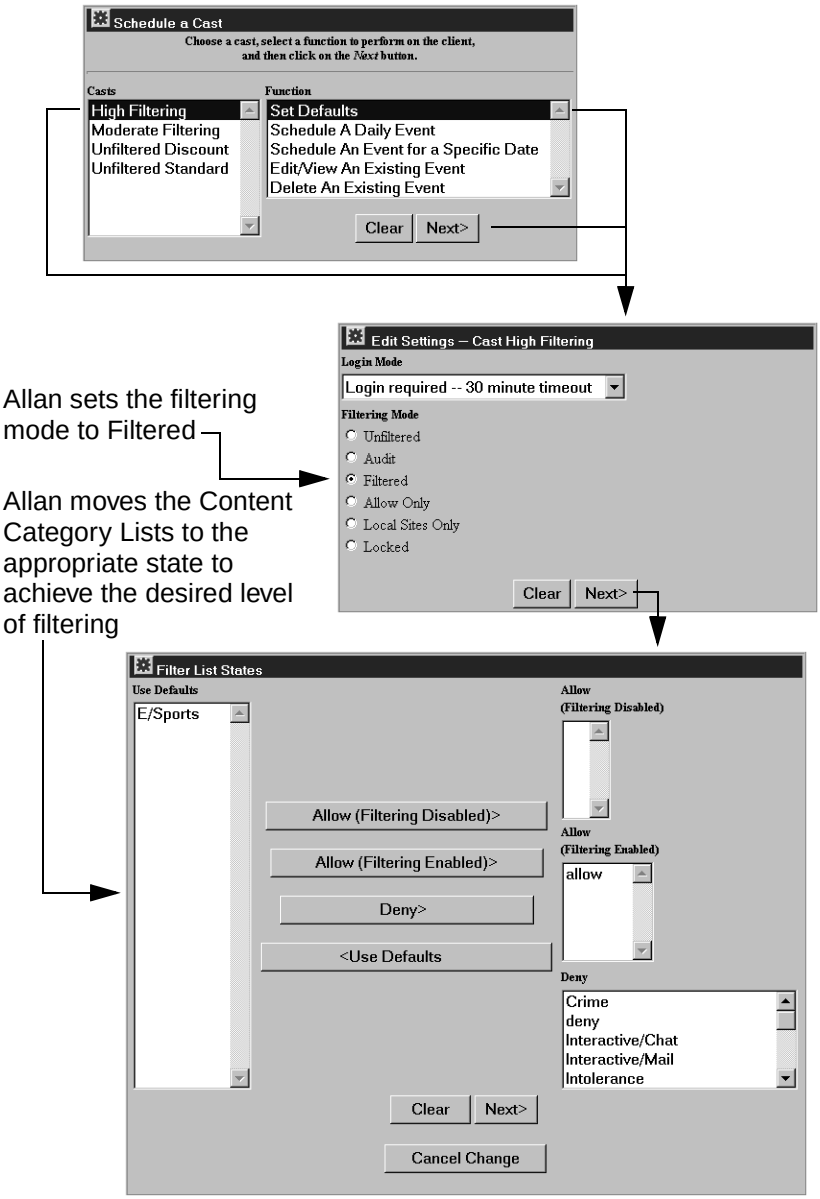
Now Allan needs to schedule the appropriate events to provide the different filtering levels. He first schedules a daily event for the Unfiltered Discount Cast to give the Users in this Cast unfiltered Internet access each day from midnight to 8:00 AM. To schedule this Cast, Allan selects the Schedule shortcut for the Cast object. From the next screen, he selects the appropriate Cast and the Schedule a Daily Event function and then clicks the **Next** button. On the next display, Allan sets the days of the week on which the event will occur (which is every day in this example) and sets the range of time for the event (midnight to 8:00

AM). He then clicks the **Next** button. From the next display, he sets the login mode to automatically log users out after 30 minutes of inactivity and selects Unfiltered as the filtering mode. He clicks the **Next** button again. I-Gear confirms that Allan's changes have been made.



Allan still needs to schedule the remaining three Casts. Because these Casts will have Internet access any time of day, Allan can simply schedule the default settings for these three Casts to establish the desired levels of filtering. To schedule the default settings for a Cast, he selects the Schedule shortcut for the Cast object. From the next display, he selects the Cast he wants to schedule and the Set Defaults function and clicks the **Next** button. He then selects the desired login and filtering modes and again clicks the **Next** button. On the next screen, he moves the Con-

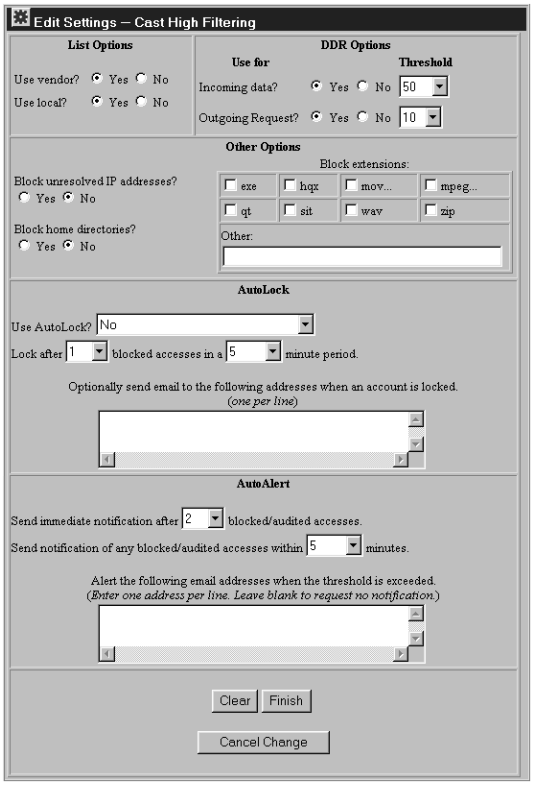
tent Category Lists to the appropriate states to achieve the desired level of filtering and then clicks the **Next** button again.



On the next screen, Allan checks the other filtering settings. He leaves the settings on this display alone for now; he feels that the default set-

tings should be adequate. He then clicks the **Finish** button. I-Gear confirms that Allan's changes have been made.

Allan leaves the default settings on this page alone →



Allan then sets the defaults for the other two Casts to reflect the appropriate levels of filtering by adjusting the List states of certain Content Category Lists and manipulating the DDR thresholds as necessary. After he finishes setting the defaults for all three Casts, he is finished configuring I-Gear. When he is ready, he can begin to populate the appropriate Casts with Users (Brightaccess.net subscribers) based on the requested level of filtering.

Index

A

Access Control Lists
  adding objects to, 53–55
  deleting objects from, 53–55
  description of, 40–42
Access denied page
  editing of, 47–48
  examples of, 14, 17
Access report. *See* Reporting
Access summary report. *See* Reporting
Add method, 5
  adding casts, 100
  adding clients, 49–50
  adding lists, 105–107
  adding users, 79–87
Administration of I-Gear
  accessing admin functions, 26, 35
  editing access denied page, 47–48
  family interface, 38–39
  standard (default) interface, 37–38
Audit mode
  definition of, 59
  example of, 154–159
AutoAlert
  activating, 65–66
  definition of, 65
  example of, 154–159
AutoLock
  activating, 63–64
  definition of, 63
  e-mail notification for, 64
  example of, 151–153
  locking methods, 63
  unlocking accounts, 63, 64

B

Backing up
  I-Gear configuration, 133–134
  restoring configuration from, 134–135
Bookmarks
  accessing, 30
  adding or deleting, 30–31

C

Cache summary report. *See* Reporting
Caching
  definition of, 3
  modifying cache config., 120–122
  setting expiration periods, 120–122
Cast object, 99–104
  adding casts, 100
  deleting casts, 100–101
  logging browsing activity for, 102–103
  modifying attributes, 102–103
  modifying membership, 101–102
  password permissions for, 102–103
  reporting on casts, 104
  scheduling casts, 104
  setting up, rules for, 99
Client object, 49–77
  adding clients, 49–50
  adding to casts, 51–53
  deleting clients, 50–51
  logging browsing activity for, 51–53
  modifying clients, 51–53
  reporting on clients, 71–77
  scheduling clients, 56–71
Client revalidation, 130–133
Content Category Lists. *See* Lists, filter

D

Debugging, enabling, 130–133
Delete method, 5
  deleting casts, 100–101
  deleting clients, 50–51
  deleting lists, 107
  deleting users, 87–88
Dictionary object, 115–117
  adding words to, 115–116
  deleting words from, 117
  modifying dictionaries, 115–117
  reporting on dictionaries, 117
Dynamic Document Review, 16–23
  changing threshold of, 62
  in conjunction with lists, 18–23
  negative scores, 116
  point values for words, 116

E

Events
  daily events, scheduling, 67–68

defaults, scheduling, 57–66
deleting existing, 71
editing existing, 70
hierarchy of, 8
specific events, scheduling, 69

F

Filter lists. *See* Lists, filter
FTP proxy
sorting feature, 33

G

Get login info from MS Proxy, 58–59
Guest mode, 58

H

History
accessing, 30
adding URLs to lists from, 108–109

L

Licensing, 125–127
List object, 105–113
adding lists, 105–107
adding URLs to, 108–109
deleting lists, 107
deleting URLs from, 109–110
modifying lists, 107–110
reporting on lists, 112–113
Lists, filter, 9–23
adding URLs to, 15–16
determining version of, 127–128
expiration of, 127–128
in conjunction with DDR, 18–23
initiating downloads, 127–128
IP addresses in for FireWall-1, 15
local lists, 13
predefined lists, 9–13
states, 13–15
Local lists. *See* Lists, filter
Logging in to I-Gear, 28
Get login info from MS Proxy, 58–59
Logging out of I-Gear, 28
Logging, browsing activity
for casts, 102
for clients, 52
for users, 88–91
system defaults for, 130–133

M

Manual, accessing online version, 27
Methods. *See also* individual methods
general description, 5
using method shortcuts, 37
Modify method, 5
modifying casts, 101–103
modifying clients, 51–53
modifying dictionaries, 115–117
modifying lists, 107–110
modifying system, 119–133
modifying users, 88–95

O

Object creation quotas
assigning at user creation, 86
assigning to users, 92–93
description of, 42–43
Objects. *See also* individual objects
administration pages for, 37
cast object, 99–104
client object, 49–77
dictionary object, 115–117
general description, 4
list object, 105–113
system object, 119–139
user object, 79–98

P

Password
cast permissions for, 102–103
changing for virtual user, 88–91
changing from tool bar, 29
system defaults for, 130–133
user permissions for, 88–91
Permissions
assigning Access Control List permissions, 55–56
assigning global permissions, 88–91
global, description of, 39
hierarchy of (by object), 6–7
Port number, changing of, 122–124
Predefined lists. *See* Lists, filter
Proxying
chaining, 119–120
definition of, 3
modifying proxy config., 119–120
other host names, 119–120
transparent, 119–120

R

RADIUS configuration, 124

Redirect timeout, 130–133

Report method, 5
- reporting on casts, 104
- reporting on clients, 71–77
- reporting on dictionaries, 117
- reporting on lists, 112–113
- reporting on the system, 136–139
- reporting on users, 96

Reporting
- access reports, 72–75
- access summary reports, 75–77
- cache summary reports, 136–139

S

Schedule method, 5
- scheduling casts, 104
- scheduling clients, 56–71
- scheduling the system, 135–136
- scheduling users, 95–96

Search capability
- for object boxes, 44–47

Showing filter settings, 31–32
- for other users, 32

Simultaneous connections, changing number of, 122–124

System object, 119–139
- client revalidation, 130–133
- debugging, 130–133
- default URL, 130–133
- enabling search capability for object boxes, 128–129
- HTTP server options, 122–124
- initiating downloads, 127–128
- licensing for I-Gear, 125–127
- logging browsing activity for, 130–133
- modifying cache config., 120–122
- modifying proxy config., 119–120
- modifying system, 119–133
- password, defaults for, 130–133
- port number changes, 122–124
- RADIUS configuration, 124
- redirect timeout, 130–133
- reporting on the system, 136–139
- scheduling the system, 135–136
- simultaneous connections, 122–124

T

Timeout, redirect, 130–133

Tool bar, 25–32
- accessing of, 25
- displaying automatically, 130–133

U

Unlocking AutoLocked accounts. *See* AutoLock

User interface. *See* Tool bar

User object, 79–98
- adding to casts, 88–91
- adding users, 79–87
- assigning Access Control List permissions to, 93
- assigning global permissions to, 88–91
- deleting users, 87–88
- disabling existing users, 87–88
- logging browsing activity for, 88–91
- modifying users, 88–91
- password permissions for, 88–91
- reenabling existing users, 95
- reporting for users, 96
- scheduling users, 95–96

User, RADIUS
- adding to I-Gear, 84–85

User, system
- adding to I-Gear, 79–81
- definition of, 79

User, virtual
- adding to I-Gear, 81–84
- changing password for, 88–91
- definition of, 79